PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Lignes directrices sur la protection des données Questions éthiques et juridiques dans la recherche et l'innovation en matière de TIC.

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) - PRINCIPES

Bud P. Bruegger (ULD)

Remerciements : L'auteur tient à remercier Giuseppe D'Acquisto, conseiller technologique principal de l'autorité italienne de protection des données (Garante per la Protezione dei Dati Personali), pour sa révision et ses suggestions.

Cette section des lignes directrices a été validée par José Luis Piñar, ancien président de l'Agence espagnole de protection des données et actuellement Cátedra Google on Privacy, Society and Innovation Universidad CEU-San Pablo, Madrid.

Ce projet a reçu un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne sous la convention de subvention n° 788039. Ce document ne reflète que le point de vue de l'auteur et l'Agence n'est pas responsable de l'usage qui pourrait être fait des informations qu'il contient.

1 Principes

La section "Comprendre la protection des données : le règlement européen en quelques mots" ci-dessus a donné un aperçu du RGPD. Elle a donc également introduit les *principes* de la protection des données, tels qu'ils figurent au chapitre 2 "Principes" du RGPD et, en particulier, à l'art. 5 "Principes relatifs au traitement des données à caractère personnel". Si *Comprendre la protection des données : le règlement européen en quelques mots* a choisi une structure qui motive le contenu du RGPD en termes de pouvoir, la présente section suit la structure de l'art. 5 du RGPD. Elle examine chaque principe de manière plus détaillée.

Les principes expriment la structure suivante :

- **Conditions relatives aux finalités** du traitement : Le type de *finalités* poursuivies par le traitement des données à caractère personnel qui sont autorisées est décrit à l'**art. 5(1)(a)** et **5(1)(b) du** RGPD. Le traitement de données personnelles à des fins qui ne satisfont pas à ces conditions n'est pas autorisé. Ces conditions sont :
    - ***Licéité*** (article 5, paragraphe 1, point a) du RGPD) ;
    - ***Légitimité*** (art. 5(1)b) du RGPD).
- **Conditions de mise en œuvre** du traitement : Lorsque la finalité répond aux critères ci-dessus, pour être autorisée, la mise en œuvre du traitement doit en outre répondre à certaines conditions. Celles-ci sont décrites à l'art. 5(1)(a) à 5(1)(f), à savoir la mise en œuvre :
    - doit être ***loyal***(article 5, paragraphe 1, point a) du RGPD) ;
    - doit être ***transparente*** (article 5, paragraphe 1, point a) du RGPD) ;
    - doit être ***limitée aux fins indiquées*** (article 5, paragraphe 1, point b) du RGPD) ;
    - doit utiliser le **minimum de données** nécessaires aux fins poursuivies (article 5, paragraphe 1, point c) du RGPD) ;
    - **ne** doit utiliser **que des données exactes** (article 5, paragraphe 1, point d) du RGPD) ;
    - doit utiliser le **degré minimal d'identification** des personnes concernées qui est nécessaire aux fins (article 5, paragraphe 1, point e) du RGPD) ;
    - doivent être **sécurisées** (article 5, paragraphe 1, point f) du RGPD).

En outre, conformément à l'art. 5(2) du RGPD, pour les responsables du traitement, se **conformer** au RGPD signifie que leur **traitement** :

- **satisfait à toutes les conditions ci-dessus** et
- les responsables du traitement sont capables de **le démontrer**.

Pour aider les lecteurs à comprendre le RGPD, la discussion détaillée des principes ci-dessus utilise la structure prévue par la loi. Cela signifie qu'un point du RGPD est discuté à la fois. **Chaque point de** l'Art. 5(1) et de l'Art. 5(2) est alors appelé un ***principe***. Le nom du principe prévu par le RGPD correspond aux titres utilisés pour les sections suivantes. Dans certains cas, plusieurs des conditions énoncées ci-dessus s'intègrent dans un seul principe.

Il existe deux exceptions à la structuration de la discussion suivante par paragraphe de l'art. 5 du RGPD. Elles sont motivées par une clarté accrue et traitent des déclarations fournies dans un paragraphe du RGPD sous le principe (c'est-à-dire le sens principal) fourni dans un autre paragraphe. À savoir, les exceptions sont les suivantes :

- l'exigence selon laquelle les finalités doivent être *spécifiques*, *explicites* et *légitimes* (prévue à l'article 5, paragraphe 1, point b) du RGPD) est examinée conjointement avec la *licéité, la loyauté et la transparence* (prévues à l'article 5, paragraphe 1, point a) du RGPD), et
- la déclaration relative à la durée de conservation se rapportant à certains types de traitement (prévue à l'art. 5(1)(e) du RGPD) est discutée avec la minimisation des données (de l'Art. 5(1)(c) du RGPD) puisqu'on peut soutenir que la période de conservation est pertinente pour que les données soient (temporairement) "*limitées à ce qui est nécessaire au regard des finalités*".

Le tableau suivant donne un aperçu de la manière dont les principes sont liés aux lettres de l'article 5 du RGPD.

	Art. 5(1)(a)	**Art. 5(1)(b)**	**Art. 5(1)(c)**	**Art. 5(1)(d)**	**Art. 5(1)(e)**	**Art. 5(1)(f)**	**Art. 5(2)**
Légitimité et **licéité**							
Loyauté							
Transparence							
Limitation de la finalité							
Minimisation des données							
Précision							
Limitation du stockage (minimisation du potentiel d'identification)							
Intégrité et **confidentialité**							
Responsabilité							

La discussion de chaque principe est structurée comme suit :

- Une **description** abstraite du principe,
- une brève discussion des **articles et des considérants du RGPD**qui permettent d'approfondir la compréhension du principe, et

- des exemples de **mesures techniques ou organisationnelles** concrètes qui peuvent être utilisées pour mettre en œuvre le principe.

La description tente de saisir l'essence du principe. La section sur les articles et considérants connexes indique les endroits du RGPD qui décrivent plus en détail comment le principe doit être appliqué concrètement. Cette section peut être parcourue rapidement lors d'une première lecture et faire l'objet d'une consultation lorsqu'une compréhension plus approfondie est souhaitée. La section sur les mesures fournit une liste non exhaustive d'exemples de la manière dont chaque principe peut être mis en œuvre dans la pratique.

Le reste de ce chapitre décrit les principes énumérés à l'art. 5 du RGPD en utilisant la structure décrite.

1.1 Licéité, loyauté et transparence

Bud P. Bruegger (ULD)

Remerciements : L'auteur remercie Iñigo de Miguel Beriain (UPV/EHU) qui a écrit une analyse de ce principe comme contribution à la description présentée ici.

Les paragraphes suivants traitent du principe de *licéité, de loyauté et de transparence* défini à l'art. 5(1)(a) du RGPD.

***Licéité, loyauté et transparence* en un coup d'œil :**

Selon le RGPD, le traitement doit être *licite* et poursuivre des *objectifs légitimes*. Il doit en outre être *équitable* et *transparent*.

La licéité est définie très précisément dans le RGPD et est atteinte si la finalité du traitement relève de l'une des six catégories (alias *bases légales*) énumérées à l'art. 6(1) du RGPD.

La légitimité est un concept beaucoup plus large, qui signifie le respect de la lettre de la loi, de l'esprit de la loi, des valeurs de la société (en particulier, la *Charte européenne des droits fondamentaux*) et des principes *éthiques*.

La loyautéest utilisée dans son acception courante. Elle interdit par exemple les pratiques manipulatrices de la part du responsable du traitement, comme le nudging. On peut dire que la plupart des articles du RGPD concernent la loyauté. Nommer le principe explicitement peut être une solution de repli dans le cas où une conséquence de l'équité ne serait pas explicitement énoncée dans le RGPD. Cela permet d'éviter toute faille.

La transparence du traitement est une stratégie principale pour équilibrer le pouvoir entre le responsable du traitement et la personne concernée. Elle fonctionne en mettant tout en lumière et en l'ouvrant ainsi à un examen minutieux. Elle est décrite dans le RGPD sous forme d'exigences détaillées concernant les informations que le responsable du traitement doit fournir aux personnes concernées et aux autorités de contrôle.

1.1.1 Description

Dans le document "Comprendre la protection des données : le règlement européen en quelques mots" ci-dessus, la plupart des propriétés requises dans ce principe ont été examinées en termes d'équilibre du pouvoir entre le responsable du traitement et les personnes concernées. Ces éléments sont résumés dans ce qui suit : Tant la *licéité* que la *légitimité* des finalités est présentée comme une condition préalable à l'autorisation du traitement. Voir "Pour quelles finalités le traitement est-il autorisé". La *loyauté* n'a pas été abordée dans l'introduction. On peut soutenir qu'en équilibrant le pouvoir entre le responsable du traitement et les personnes concernées, l'ensemble du RGPD concerne la loyauté. La *transparence* a été présentée comme une condition préalable à la responsabilité. Voir "Les responsables du traitement sont pleinement responsables" pour plus de détails.

Le RGPD définit ce principe comme suit :

Définition de l'art. 5(1)(a) du RGPD :

Les données à caractère personnel sont traitées de manière **licite**, **équitable** et **transparente** à l'égard de la personne concernée ("*licéité, loyauté et transparence*") ;

La licéité, la loyauté et la transparence sont examinées plus en détail dans les paragraphes qui suivent.

1.1.1.1 Condition préalable à la licéité : des objectifs précis et explicites

La licéité est une exigence pour les finalités du traitement[62] . Il est donc impossible de raisonner à son sujet sans connaître au préalable les finalités précises qui sont poursuivies par le traitement. Pour cette raison, l'exigence de l'**art. 5, paragraphe 1, point b),** selon laquelle les finalités doivent être précisées et explicites, est examinée ici en tant que condition préalable :

Les données à caractère personnel sont collectées pour des **finalités spécifiques, explicites** et légitimes.

Finalités spécifiques :

Le *groupe de travail Article 29 sur la protection des données* écrit[63] :

> "La **spécification de la finalité est au cœur du cadre juridique** établi **pour la protection des données à caractère personnel**. Afin de **déterminer si le traitement des données est conforme à la loi** et d'établir quelles garanties en matière de protection des données doivent être appliquées, il est **indispensable d'identifier la ou les finalités spécifiques** pour lesquelles la collecte de données à caractère personnel est requise."

[62] Il n'entre pas dans le cadre du présent document de fournir une analyse juridique approfondie de la notion de finalité au-delà de sa signification dans le langage courant. Il convient simplement de souligner que les finalités du traitement sont généralement liées à un objectif que le responsable du traitement poursuit. Ces objectifs doivent être concrets (plutôt que théoriques) et il est souvent possible de déterminer si l'objectif a été atteint ou de mesurer dans quelle mesure il l'a été.

[63] Surlignage ajouté par l'auteur, pour la citation, voir page 15 de : Groupe de travail Article 29 sur la protection des données, 00569/13/FR, WP203, Avis 03/2013 sur la limitation de la finalité, adopté le 2 avril 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (dernière visite le 27/05/2020).

La spécification peut être considérée comme la première tâche de la conceptualisation d'une activité de traitement qui guide toutes les décisions ultérieures, notamment :

- si le **traitement est permis**, c'est-à-dire licite et légitime,
- **ce qu'implique la mise en œuvre** du traitement nécessaire à la réalisation des finalités, et
- quelles **garanties en matière** de protection des données doivent être appliquées.

Le *groupe de travail* déclare en outre :[64]

> "La **finalité** de la collecte doit être **clairement** et **spécifiquement** identifiée : elle doit être suffisamment **détaillée** pour déterminer quel type de traitement est et n'est pas inclus dans la finalité spécifique, et pour permettre que le respect de la loi soit évalué et que des garanties de protection des données soient appliquées."

et

> "Pour ces raisons, **une finalité vague ou générale**, comme par exemple "l'amélioration de l'expérience des utilisateurs", "des fins de marketing", "des fins de sécurité informatique" ou "des recherches futures "**ne répondra** généralement **pas** - sans plus de détails - aux **critères de *spécificité.*"**

Des objectifs explicites :

Le groupe de travail déclare en outre :[65]

> "Les données à caractère personnel doivent être collectées pour des **finalités explicites**. Les finalités de la collecte **ne** doivent **pas seulement** être précisées dans l'**esprit** des personnes responsables de la collecte des données. Elles doivent également être rendues explicites. En d'autres termes, elles doivent être **clairement révélées, expliquées ou exprimées sous une forme intelligible**."

Notez que l'obligation de rendre les finalités explicites est étroitement liée à l'information des personnes concernées sur les finalités du traitement (voir art. 13(1)(c) et 14(1)(c) du RGPD).

Sur la base de la condition préalable de la spécification des finalités explicites, la légitimité et la licéité peuvent être discutées.

1.1.1.2 Légitimité et légalité

Alors que l'art. 5(1)(a) du RGPD ne parle que de *licéité*, l'exigence étroitement liée de *légitimité* est énoncée à l'art. 5(1)(b) du RGPD. Étant donné que tous deux expriment des exigences concernant les finalités du traitement, ils sont examinés ici ensemble.

L'art. 5(1)(b) du RGPD stipule :

> Les données à caractère personnel sont collectées pour des **finalités** *spécifiques, explicites* et **légitimes** et [...]

Le RGPD ne fournit pas de définition de la *légitimité*, mais le *groupe de travail Article 29 sur la protection des données* fournit la suivante :[66]

> L'exigence de ***légitimité*** signifie que les objectifs doivent être **"conformes à la loi" au sens le plus large**. Cela inclut **toutes les formes de droit écrit et de common law**, la **législation**

[64] WP203, page 15, surlignage ajouté par l'auteur.
[65] WP203, page 17, surlignage ajouté par l'auteur.
[66] WP203, page 20, , surlignage ajouté par l'auteur.

primaire et secondaire, les **décrets municipaux**, les **précédents** judiciaires, les **principes constitutionnels**, les **droits fondamentaux**, les **autres principes juridiques**, ainsi que la **jurisprudence**, telle que cette "loi" serait interprétée et prise en compte par les tribunaux compétents.

La légitimité est donc une **exigence** très **large**. Cela devient encore plus significatif si l'on considère que certaines législations, telles que le *règlement sur les essais cliniques*[67] , incluent également des ***exigences éthiques***. Mais même lorsque l'éthique n'est pas prescrite par la loi, il existe un risque que des finalités clairement contraires à l'éthique soient considérées comme également illégitimes. Ce peut être le cas, par exemple, lorsque le traitement a lieu au mépris de la désapprobation d'un comité d'éthique de la recherche.

Contrairement à la *légitimité*, la ***licéité*** est en effet définie dans le RGPD. L'**art. 6(1) du** RGPD est ainsi rédigé :

Le traitement n'est **licite** que si et dans la mesure où au moins une des conditions suivantes s'applique : [...]

Dans l'omission représentée par [...], six *bases dites légales* possibles sont énumérées. Elles peuvent être considérées comme des catégories de finalités. Elles sont décrites plus en détail dans la section "Articles et récitals connexes considérants connexes" ci-dessous.

1.1.1.3 Loyauté

On peut dire que l'ensemble de la protection des données, et donc le RGPD, concerne la loyauté envers les personnes concernées. Le RGPD peut être considéré comme précisant ce que signifie réellement et concrètement la *loyauté*.

Sa mention explicite en tant que principe peut donc être considérée comme une "clause de repli" pour le cas où une exigence concrète de loyauté n'a pas été explicitement énoncée dans le RGPD. Même dans ce cas, le principe de *loyauté* empêcherait toute "faille" dans le RGPD.

Bien que l'on puisse considérer que l'ensemble du RGPD concerne la loyauté, la section "Articles et récitals connexes considérants connexes" ci-dessous donne quelques exemples où la loyauté est particulièrement évidente.

1.1.1.4 Transparence

La transparence est un concept bien compris et constitue une condition préalable essentielle à la responsabilisation dans le cadre du RGPD. L'objectif principal de la transparence est d'informer les **personnes concernées** dès le départ[68] de l'existence du traitement et de ses principales caractéristiques. D'autres informations (telles que les données relatives à la personne concernée) sont disponibles sur demande. Les personnes concernées doivent également être informées de certains événements, notamment des violations de données (dans le cas où la personne concernée est exposée à un risque élevé). La transparence est également soutenue par la désignation par les responsables du traitement d'un délégué à la protection des données qui fait office de point de contact unique pour les préoccupations des personnes concernées. Dans le RGPD, les personnes concernées sont habilitées à être les principaux

[67] RÈGLEMENT (UE) n° 536/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE, https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf (dernière visite le 27/05/2020).

[68] L'expression "en amont" signifie que les personnes concernées doivent être informées du traitement avant qu'il n'ait lieu. Elle n'implique pas une certaine méthode de fourniture d'informations et n'exclut pas les moyens dynamiques de fournir les informations nécessaires.

gardiens de leurs propres droits et libertés. De toute évidence, la transparence est une condition préalable à la détection et à l'intervention en cas de non-conformité.

Les autorités de contrôle, comme leur nom l'indique, sont également les gardiennes du respect du RGPD, même si leur intervention est souvent déclenchée par des plaintes déposées par des personnes concernées[69] . Il existe des exigences de transparence pour les responsables du traitement qui visent spécifiquement les contrôleurs, notamment les registres de traitement (voir "Documentation du traitement" dans la section "Principaux outils et actions" de la partie II) et les analyses d'impact sur la protection des données (voir la section du même nom dans "Principaux outils et actions", partie II des présentes lignes directrices). Le fait que les responsables du traitement soient responsables[70] devant les autorités de contrôle et qu'ils doivent permettre des enquêtes et des audits sur place [71][72] renforce la transparence.

1.1.2 Articles et récitals connexes

1.1.2.1 Licéité

La définition de la licéité est donnée à l'art. 6(1) du RGPD. Elle se lit comme suit :

> Le traitement **n'est *licite* que si et dans la mesure où** au moins une des conditions suivantes s'applique :
>
> (a) les personnes concernées ont donné leur **consentement** au traitement de leurs données personnelles pour une ou plusieurs *finalités* spécifiques ;
>
> (b) le traitement est nécessaire à l'**exécution d'un contrat** auquel la personne concernée est partie ou pour prendre des mesures à la demande de la personne concernée préalablement à la conclusion d'un contrat ;
>
> (c) le traitement est nécessaire au **respect d'une obligation légale** à laquelle le responsable du traitement est soumis ;
>
> (d) le traitement est nécessaire à la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique ;
>
> (e) le traitement est nécessaire à l'exécution d'une mission d'**intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
>
> (f) le traitement est nécessaire aux *finalités* des **intérêts légitimes poursuivis par le responsable du traitement** ou par un tiers, **à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée** qui exigent la protection des données à caractère personnel, en particulier lorsque la personne concernée est un enfant.
>
> Le premier alinéa, point f), ne s'applique pas aux traitements mis en œuvre par les autorités publiques dans l'exercice de leurs missions.

Alors que les finalités du traitement doivent être spécifiques et explicites (voir art. 5(1)(b), et donc également suffisamment étroites et spécifiques, les finalités ci-dessus sont clairement des **catégories de finalités**. (Lorsque le mot finalité a été utilisé explicitement, il est donc

[69] Voir l'art. 57(1)(f) du RGPD.
[70] Voir l'art. 58(1)(a) du RGPD.
[71] Voir l'art. 58(1)(f) du RGPD.
[72] Voir l'art. 58(1)(b) du RGPD.

écrit en italique). Elles sont communément appelées ***bases légales***[73] et sont référencées par leur position dans l'article 6 ; par exemple, le *consentement* serait alors la *base légale* de l'art. 6(1)(a).

Le RGPD prévoit deux articles qui énoncent des **exigences supplémentaires en matière de licéité** pour deux cas différents : les **données sensibles** et les données relatives aux **condamnations pénales**. Il s'agit en particulier des articles suivants :

L'art. 9 du RGPD stipule que le traitement de données particulièrement sensibles est en principe interdit et énumère 10 exceptions à cette règle. Ces exceptions ont une structure comparable à celle des bases légales de l'art. 6. L'article précise que les données sont particulièrement sensibles, si elles révèlent :

- l'origine raciale ou ethnique,
- les opinions politiques,
- les croyances religieuses ou philosophiques,
- l'adhésion à un syndicat,

ou sont :

- les données génétiques,
- des données biométriques dans le but d'identifier de manière unique une personne physique,
- des données concernant la santé, ou
- les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Pour ces données, des exigences plus strictes s'appliquent afin que leur traitement soit considéré comme licite. Par exemple, au lieu du simple consentement de l'art. 6(1)(a), le traitement de ces données sensibles requiert un niveau de consentement plus exigeant appelé ***consentement explicite*** (voir l'art. 9(2)(a) du RGPD).

Comme l'art. 9 pour les données particulièrement sensibles, l'**art. 10 du RGPD** restreint davantage le traitement des "données relatives aux **condamnations pénales et aux infractions** ou aux mesures de sûreté connexes". En particulier, pour être licite, le traitement doit être "effectué uniquement sous le **contrôle de l'autorité publique** ou lorsqu'il est autorisé par le droit de l'Union ou des États membres, moyennant des garanties appropriées pour les droits et libertés des personnes concernées".

Il existe plusieurs articles et considérants dans le RGPD qui précisent le **concept de consentement** (de l'art. 6(1)(a) du RGPD) de manière plus détaillée. Les plus importants sont les suivants :

- **L'art. 4(11)** qui **définit le consentement** ;
- **L'art. 7** qui énumère les **conditions du consentement**
- **L'art. 8** qui régit les **conditions applicables au consentement de l'enfant en ce qui concerne les services de la société de l'information.**

[73] Le terme "*base légale*" est largement utilisé dans le RGPD et est recommandé ici comme terme préférentiel. Alternativement, le RGPD contient également le terme *legal ground*. Dans la littérature, le terme *base juridique* est également utilisé.

Considérant que le consentement est un concept complexe, le **Conseil européen de la protection des données** a publié des ***lignes directrices*** *05/2020* faisant autorité ***sur le consentement*** *en vertu du règlement 2016/679*[74] .

Outre le *consentement*, la notion d'***intérêt légitime poursuivi par le responsable du traitement*** (de l'art. 6(1)(f) du RGPD) est difficile à comprendre pleinement. Ce qui est crucial ici, c'est la restriction "**sauf si** ces intérêts sont supplantés par les intérêts ou les libertés et droits fondamentaux de la personne concernée". Cela signifie que l'intérêt légitime du responsable du traitement doit être mis en balance avec les intérêts des personnes concernées. Pour déterminer si tel est le cas, le responsable du traitement doit procéder à un "***test de mise en balance"***. La manière de procéder est décrite dans la section "Principaux outils et actions" de la partie II des présentes lignes directrices. Elle se fonde principalement sur l'*avis 06/2014* du *groupe de travail Article 29,* qui fait autorité, *sur la notion d'intérêt légitime du responsable du traitement des données au titre de l'article 7 de la directive 95/46/CE*[75] . Bien que cet avis soit fondé sur la directive sur la protection des données qui a précédé le RGPD, il est en général applicable à l'interprétation de l'art. 6(1)(f) du RGPD. Il est recommandé pour une **lecture complémentaire** sur le sujet.

1.1.2.2 Loyauté

On peut dire que l'ensemble du RGPD concerne la loyauté. Voici quelques articles du RGPD qui l'illustrent particulièrement bien.

Un domaine où la loyauté est évidente concerne les exigences de transparence. Ici, l'**art. 12(1)** stipule que les responsables du traitement doivent fournir les informations "à la personne concernée sous une forme **concise**, transparente, **intelligible** et **aisément accessible**, en utilisant **un langage clair et simple**, en particulier pour toute information destinée spécifiquement à un enfant." De toute évidence, cela interdit la pratique déloyale consistant à fournir les informations requises sous une forme inaccessible aux personnes concernées.

De même, le **consentement** ne peut pas être implicite, mais nécessite plutôt une "déclaration ou une **action positive claire**" (voir l'**art. 4(11)** du RGPD). Le même article précise en outre que le consentement doit être **donné librement**, **spécifique**, **éclairé** et **sans ambiguïté**". En outre, à **tout moment,** sans besoin de justification, une personne concernée doit pouvoir **retirer son** consentement **aussi facilement qu'il a été donné**. Ces exigences strictes en matière de consentement interdisent directement de nombreuses pratiques manipulatrices, notamment le "nudging"[76] des personnes concernées.

Plusieurs **droits des personnes concernées** peuvent être directement associés à la loyauté. Il s'agit notamment de :

- Le **droit de rectification** (article 16 du RGPD) pour éviter que les personnes concernées ne subissent des conséquences négatives en raison de données inexactes ;
- Le **droit à la limitation du traitement** (article 18 du RGPD) qui empêche les responsables du traitement d'utiliser davantage les données qui ont été signalées

[74] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0, Adopté le4 mai2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (dernière visite le 22/05/2020).

[75] Groupe de travail Article 29 sur la protection des données, 844/14/FR, WP217, Avis 06/2014 sur la notion d'intérêt légitime du responsable du traitement des données au titre de l'article 7 de la directive 95/46/CE, adopté le 9 avril 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (dernière visite le 22/05/2020).

[76] Voir par exemple, Weinmann, M., Schneider, C. & Brocke, J.v. Digital Nudging. Bus Inf Syst Eng 58, 433-436 (2016). https://doi.org/10.1007/s12599-016-0453-1 (dernière visite le 22/05/2020).

comme étant inexactes ou se rapportant à un traitement auquel la personne concernée s'est opposée ;

- Le **droit à la portabilité des données** (article 20 du RGPD) qui permet d'éviter les situations de verrouillage et une éventuelle perte (par exemple, d'investissement[77]) lorsque les utilisateurs changent de relation avec le responsable du traitement ;
- Le **droit d'opposition** (art. 21 du RGPD) lorsque, dans le cas d'une base légale de l'art. 6(1)(f) du RGPD, les personnes concernées peuvent présenter **leurs situations spécifiques** dans lesquelles leur intérêt prévaut sur les intérêts légitimes du responsable du traitement ;
- Le **droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé** (art. 22duRGPD), qui prévoit également le **droit d'obtenir une intervention humaine** de la part du responsable du traitement (voir paragraphe 3).

Une autre indication de la loyauté est que le responsable du traitement doit prendre en considération le point de vue des personnes concernées. Cela est par exemple évident dans le considérant 50 du RGPD qui exige de prendre en compte les attentes raisonnables des personnes concernées lorsqu'il s'agit de déterminer si une finalité est compatible avec l'art. 6(4). Cela apparaît également dans les analyses d'impact sur la protection des données (article 35 du RGPD), où les responsables du traitement doivent, le cas échéant, demander l'avis des personnes concernées ou de leurs représentants (article 35, paragraphe 9, du RGPD).

1.1.2.3 Transparence

Plusieurs articles du RGPD apportent des précisions sur le principe de *transparence*. Il s'agit notamment des articles suivants :

- Les **articles 12 à 14** décrivent en détail les **informations** que les responsables du traitement doivent fournir **d'emblée** aux personnes concernées.
- **L'art. 15** décrit les informations qui doivent être fournies sur demande des personnes concernées, y compris l'accès complet à leurs données.
- **L'art. 34** décrit comment les personnes concernées doivent être informées des violations de données, lorsque celles-ci sont susceptibles d'entraîner un risque élevé.
- **L'art. 38(4)** désigne le *délégué à la protection des données* du responsable du traitement comme point d'accès pour les personnes concernées.
- **Les art. 12** et **19** décrivent les informations que les responsables du traitement doivent fournir aux personnes concernées qui exercent un de leurs droits.
- **Les art. 30 - *Registres de traitement*** et **35 –*Analyse d'impact sur la protection des données*** décrivent les informations qui doivent être fournies aux autorités de contrôle. (Ces dernières uniquement si le traitement est susceptible d'entraîner un risque élevé).
- **L'art. 58(1)** précise comment les responsables du traitement doivent être transparents vis-à-vis des autorités de contrôle en étant responsables (point a), en autorisant les inspections et les audits (point b) et en donnant accès à leurs locaux (point f).
- **L'art. 33** décrit la notification des violations aux autorités de contrôle.

[77] La collection de photos personnelles est un bon exemple de perte d'investissement possible.

Compte tenu de l'importance de la transparence dans le RGPD, le **Conseil européen de la protection des données** a fourni une interprétation faisant autorité des obligations connexes dans ses **Lignes directrices sur la transparence** en vertu du règlement 2016/679 (wp260rev.01)[78] . La lecture de ce document est recommandée.

1.1.3 Mesures techniques et organisationnelles connexes

Des exemples de mesures visant à mettre en œuvre différents aspects du principe sont fournis ci-après.

1.1.3.1 Légitimité et licéité

- Au moins lorsque la vérification et la démonstration de la **légitimité** nécessitent des **étapes formelles**, celles-ci peuvent être considérées comme des mesures organisationnelles de soutien à la légitimité. La **demande et l'approbation** de certaines recherches médicales par le **comité d'éthique de la recherche** compétent en sont un bon exemple.
- **La spécification d'objectifs explicites est une** condition préalable à l'évaluation de la légitimité et de la licéité. Cette condition peut être considérée comme une mesure en soi, en particulier lorsqu'elle s'accompagne de **réflexions** sur la manière de rendre la spécification **aussi spécifique** et **étroite que possible**. Dans ce cas, une telle analyse peut également être considérée comme faisant partie de cette mesure.
- La principale mesure à l'appui de la licéité consiste à identifier une ou plusieurs **bases légales** de l'**art. 6(1)** du RGPD. Dans de nombreux cas, une activité de traitement utilise plusieurs bases légales. Un cas d'utilisation[79] publié par le *Data Privacy Vocabulary Community Group* du W3C fournit un exemple facilement accessible.
- Lorsque l'art. **6, paragraphe 1, point a)** du RGPD, c'est-à-dire le *consentement,* a été choisi comme base légale, une **analyse** qui justifie que les **exigences** strictes du RGPD **en matière de consentement (librement donné et éclairé)** ont été respectées est une mesure importante. Il peut s'agir, par exemple, de vérifier si les informations fournies comme base du consentement sont effectivement compréhensibles pour les personnes concernées et si le retrait du consentement est effectivement aussi facile que de le donner.
    - En outre, lorsque des **enfants** ou d'autres **personnes vulnérables** sont concernés, cette analyse doit mettre l'accent sur les garanties relatives à l'art. 7 du RGPD.
- Lorsque l'art. **6, paragraphe 1, point f)**du RGPD, c'est-à-dire le *consentement légitime du responsable du traitement,* a été choisi comme base légale, les mesures comprennent une spécification précise des intérêts légitimes, ainsi qu'un ***test de mise en balance*** (voir la section du même nom dans "Principaux outils et actions" de la partie II des présentes lignes directrices) pour vérifier que ceux-ci prévalent effectivement sur les intérêts, les droits et les libertés des personnes concernées.

---

[78] EDPB, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (dernière visite le 22/05/2020).

[79] Bruegger, Schlehahn & Zwingelberg, Data Privacy Vocabulary Community Group, Data Protection Aspects of Online Shopping - A Use Case, https://www.w3.org/community/dpvcg/2019/12/12/data-protection-aspects-of-online-shopping-a-use-case/ (dernière visite le 25/05/2020).

- Quelle que soit la base légale, lorsque les responsables du traitement ont l'intention de **traiter** certaines données **plus avant,** au-delà des finalités initiales, à des **fins compatibles** (voir l'art. 5(1)(b) du RGPD), l'analyse fondée sur les critères de l'art. 6(4) pour démontrer que ces finalités supplémentaires sont effectivement compatibles, est une mesure qui démontre la licéité de ce traitement.
- Si des catégories particulières de données (c'est-à-dire des données sensibles), ou des données relatives à des condamnations pénales, sont traitées, des mesures supplémentaires doivent être prises en plus de celles relatives à l'art. 6(1) du RGPD. En particulier, dans le premier cas, la condition de l'art. 9(2) du RGPD, pour laquelle une exception à l'interdiction de traiter des données sensibles s'applique, doit être trouvée et documentée. Dans le second cas, les conditions qui rendent le traitement admissible conformément à l'art. 10 du RGPD doivent être mises en œuvre et documentées.

1.1.3.2 Loyauté

- Comme cela a été expliqué ci-dessus, toutes les exigences du RGPD peuvent être considérées comme une question de loyauté ; plusieurs droits des personnes concernées ont toutefois été présentés comme particulièrement pertinents. Les principales mesures en faveur de la loyauté sont donc une **mise en œuvre** adéquate **des droits des personnes concernées**.

1.1.3.3 Transparence

- La mise en œuvre des exigences des art. 12 à 14 du RGPD pour fournir des **informations** adéquates et facilement compréhensibles **aux personnes concernées** est une mesure primordiale pour soutenir la transparence.
- Il en va de même pour les documents préparés pour informer les autorités de contrôle, en particulier les ***registres de traitement*** (conformément à l'article 30 du RGPD) et une ***analyse d'impact sur la protection des données*** (conformément à l'article 35 du RGPD). Une autre mesure est la publication partielle de cette analyse d'impact.
- Toute analyse qui évalue l'efficacité et l'accessibilité des informations fournies - éventuellement en ce qui concerne des catégories particulières de personnes concernées comme les enfants - peut être considérée comme une mesure en soi.
- La nomination d'un délégué à la protection des données peut en partie être considérée comme une mesure visant à accroître la transparence tant à l'égard des personnes concernées que de l'autorité de contrôle.

1.2 Limitation de l'objet

Bud P. Bruegger (ULD)

Remerciements : Les auteurs remercient la contribution d'Iñigo de Miguel Beriain (UPV/EHU) qui a écrit une analyse de ce principe comme contribution à la description présentée ici.

Les paragraphes qui suivent traitent du principe de *limitation de la finalité* qui est défini à l'art. 5(1)(b) du RGPD.

***Limitation de l'objet* en un coup d'œil :**

Les données qui ont été **collectées pour des finalités "initiales" spécifiques ne peuvent être traitées ultérieurement** :

- pour ces **finalités initiales**, ou pour
- **des finalités de compatibilité**.

Pour le cas général, le RGPD donne des **critères** sur la manière de **déterminer la compatibilité** des finalités (voir art. 6(4)). En outre, certaines finalités sont **préapprouvées comme étant compatibles** par le RGPD (voir art. 5(1)(b)) pour autant que des garanties appropriées soient mises en œuvre (voir l'article 89). Il s'agit notamment de :

- **l'archivage** dans l'**intérêt public,**
- **la recherche scientifique ou historique**, et
- **les statistiques**.

1.2.1 Description

Dans la section "Comprendre la protection des données : le règlement européen en quelques mots" ci-dessus, la *limitation de la finalité* était motivée par le fait de restreindre l'utilisation du pouvoir acquis exclusivement à la réalisation des finalités déclarées et légitimes. (Voir la section "1.6.4 Limiter les responsables du traitement à l'utilisation du pouvoir uniquement pour réaliser les finalités légitimes déclarées" pour plus de détails).

Le RGPD définit ce principe comme suit :

Définition de l'art. 5(1)(b) du RGPD :

Les données à caractère personnel sont collectées pour des finalités spécifiques, explicites et légitimes et **ne sont pas traitées ultérieurement** de **manière incompatible avec ces finalités** ; [...] ("*limitation de la finalité*") ;

Notons que la première moitié de cette phrase a déjà été discutée dans le cadre du principe précédent. En particulier, l'exigence de ***spécificité* et d'*explicitation des*** finalités est une **condition préalable pour pouvoir** parler de ***licéité*** ; l'exigence de légitimité concerne les buts et a donc été discutée avec la *licéité*.

Ce qui est discuté ici plus en détail est l'essence de ce principe, à savoir la **limitation au traitement compatible avec les finalités**. Il s'agit d'une exigence concernant la mise en œuvre de l'activité de traitement, et non les finalités.

1.2.1.1 Ne pas être traité d'une manière incompatible avec ces finalités.

L'essentiel de ce principe est donc contenu dans la demi-phrase "ne pas être traité ultérieurement d'une manière incompatible avec ces finalités". Cette phrase est analysée plus en détail dans ce qui suit.

La phrase parle de compatibilité avec les **finalités**. Il ressort clairement de la première moitié de la phrase qu'il s'agit des finalités **qui ont été explicitement spécifiées**[80] (voir la section 1.1.1.1 ci-dessus). La partie de l'art. 5(1)(b) qui a été représentée par [...] et qui sera discutée ci-dessous utilise également le concept de "compatibilité avec les ***finalités initiales"***. Les *finalités initiales* semblent donc être les mêmes que celles spécifiées (lors de la conception de l'activité de traitement).

L'art. 5(1)(b) exprime ainsi, que le traitement doit être compatible avec :

- les finalités **initiales elles-mêmes**, ou
- **d'autres finalités compatibles** avec ces finalités initiales.

La première découle du raisonnement selon lequel les buts sont toujours compatibles avec eux-mêmes.

Le libellé de l'art. 5(1)(b) parle de "traitement **ultérieur**". Bien que cela puisse être compris de manière temporaire, c'est-à-dire dans le sens de "après que les finalités initiales ont été réalisées", l'aspect temporel ne semble pas pertinent pour ce principe. Au contraire, "ultérieur" a le sens de "au-delà" sans signification temporelle et se réfère purement aux objectifs. La situation est visualisée dans Figure 1:

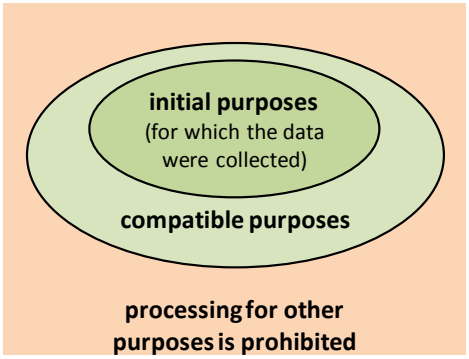

Figure 1: Le traitement est autorisé à des finalités initiales et compatibles.

Il est important de savoir qu'aucune base légale supplémentaire n'est nécessaire pour poursuivre le traitement à des fins compatibles. Cela est indiqué explicitement dans le considérant 50 du RGPD (2nd phrase). En ce qui concerne le traitement ultérieur à des fins compatibles, il est indiqué :

> Dans ce cas, aucune base légale distincte de celle qui a permis la collecte des données personnelles n'est requise.

1.2.1.2 Utilisation à des fins incompatibles

Cela soulève la question de savoir comment il peut arriver de traiter des données personnelles à des fins incompatibles et quelles en sont les conséquences.

Il est important de comprendre comment le traitement peut se produire pour pouvoir l'éviter. Les trois exemples suivants illustrent le problème sans prétendre à l'exhaustivité :

[80] Ce sont également les finalités qui sont communiquées aux personnes concernées, comme l'exigent les art. 13 et 14 du RGPD).

- **La dérive fonctionnelle** : il est courant que les activités de traitement évoluent au fil du temps. Il est également courant qu'elles acquièrent alors de nouvelles fonctionnalités ou "caractéristiques" qui correspondent à un traitement supplémentaire ou modifié. Dans les cas où le responsable du traitement n'exerce pas un contrôle suffisant sur cette évolution, le traitement peut passer inaperçu au-delà des finalités initiales ou compatibles.
- **Absence de séparation** : Supposons qu'un responsable du traitement exerce plusieurs activités de traitement indépendantes qui poursuivent des finalités distinctes. Si le responsable du traitement ne met pas en œuvre des mesures adéquates pour séparer les différentes activités de traitement, il est facile que les données collectées pour une série de finalités soient utilisées pour d'autres finalités. Ceci est illustré dans Figure .

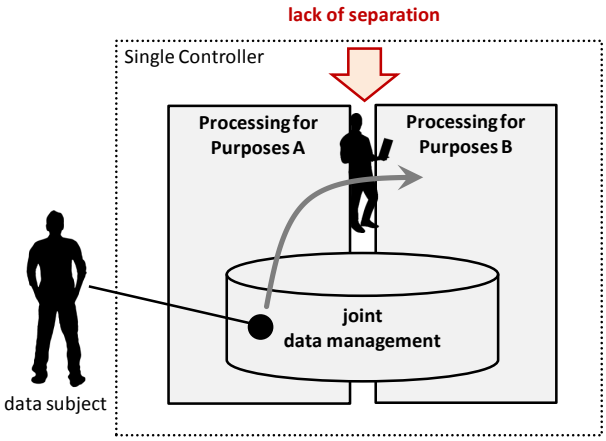

Figure 2: L'absence de séparation conduit à l'utilisation de données à des fins incompatibles.

- **Les destinataires qui ont leurs propres finalités**: Les destinataires sont des personnes ou des organisations auxquelles des données à caractère personnel sont divulguées (voir la définition à l'art. 4(9) du RGPD). Les destinataires peuvent par exemple être :
    - **les employés** qui accèdent *légitimement* aux données sur instruction du responsable du traitement pour des finalités compatibles du traitement, ou
    - **des attaquants externes** qui accèdent illégitimement aux données par le biais d'une brèche[81] .

  Dans ce dernier cas, il est évident que le destinataire utilise les données à caractère personnel à d'autres fins. Ce sont ces mêmes finalités qui ont probablement motivé l'attaque en premier lieu. Mais même les employés peuvent avoir d'autres intérêts dans les données que les finalités déclarées de leur employeur. Le cas où l'employé connaît déjà la personne concernée et apprend des informations qui ne seraient pas accessibles autrement en est un bon exemple.

Avec la compréhension acquise à partir de ces exemples qui illustrent comment les données peuvent être utilisées avec d'autres finalités, la question des conséquences possibles doit être posée.

Dans tous les cas, les principes **fondamentaux** de *licéité* et de *légitimité* sont susceptibles d'être **violés**. Selon ces principes, le traitement est interdit à moins qu'il ne soit justifié par une licéité et une légitimité démontrées des finalités. Ce n'est évidemment pas le cas lorsque le traitement est effectué pour des finalités incompatibles, et donc injustifiées.

[81] Les contrôleurs ne sont pas responsables des actions des attaquants, mais seulement de la prévention des attaques par des mesures de sécurité adéquates.

L'utilisation des données en dehors et au-delà des finalités justifiées **permet** également aux **responsables du traitement** malhonnêtes d'**accumuler du pouvoir**. Cela peut se produire, par exemple, lorsque les responsables du traitement combinent les ensembles de données de personnes dans le cadre d'activités de traitement distinctes, conservent et accumulent des données alors qu'elles ne sont plus nécessaires aux fins poursuivies, voire acquièrent des données auprès d'autres sources afin d'accroître leur pouvoir sur les personnes concernées. Ce pouvoir accumulé dépasse manifestement le gain de pouvoir qui était justifié par la démonstration de la licéité et de la légitimité des finalités initiales.

Il est évident qu'au-delà de la seule violation des principes de protection des données, en fonction des finalités pour lesquelles les données sont utilisées ou violées, les **personnes concernées** peuvent également subir des **dommages matériels ou immatériels**. Par exemple, la connaissance de certaines données relatives à la santé peut affecter de manière significative des relations lorsqu'elles sont accessibles à des connaissances ou empêcher des opportunités d'emploi lorsqu'elles sont accessibles à des employeurs potentiels. Lorsqu'ils sont utilisés à des fins criminelles, certains types de données peuvent servir de base à un chantage.

1.2.1.3 Quand les objectifs sont-ils compatibles ?

Les paragraphes suivants traitent de la manière de déterminer si d'éventuels objectifs supplémentaires sont considérés comme compatibles. Ils s'appuient principalement sur l'art. 6(4) du RGPD.

Dans le cas où une **base légale** de ***consentement*** (voir l'art. 6(1)(a) du RGPD) a été choisie pour le traitement, tout traitement ultérieur à des **fins supplémentaires** autres que celles compatibles approuvées au préalable (voir ci-dessous) **est considéré comme incompatible**[82] . Cela s'explique par le fait que le consentement est toujours propre aux finalités spécifiques[83] . Il serait manifestement injuste et non transparent d'"élargir" les finalités du traitement au-delà des finalités spécifiques auxquelles la personne concernée a consenti.

L'art. 6(4) prévoit ensuite les **critères** suivants que les responsables du traitement doivent utiliser pour déterminer si une finalité supplémentaire est compatible (légèrement reformulé par rapport au RGPD) :

(a) Tout **lien entre** les **finalités initiales** et les **finalités supplémentaires** envisagées ;

(b) le **contexte dans lequel les données** à caractère personnel ont **été collectées**, notamment en ce qui concerne la **relation** entre les **personnes concernées** et le **responsable du traitement** ;

(c) la **nature des données à caractère personnel**, en particulier si elles comprennent des **catégories particulières de données à** caractère personnel (c'est-à-dire des **données** sensibles) ou si des données à caractère personnel liées à des **condamnations pénales** et à des **infractions** sont traitées ;

(d) les **conséquences possibles** du traitement ultérieur envisagé **pour les personnes concernées** ;

(e) l'**existence de garanties appropriées**, qui peuvent inclure la **pseudonymisation**.

[82] Notez que l'art. 6(4) du RGPD sur les finalités compatibles exclut explicitement qu'il soit applicable lorsque la base juridique est le consentement.

[83] En particulier, ces finalités sont spécifiées dans le dialogue qui demande le consentement et cette spécification est un aspect important du caractère éclairé du consentement.

Des orientations supplémentaires, y compris des exemples d'application de ces critères, sont disponibles auprès du *groupe de travail Article 29 sur la protection des données*[84] . Bien que cet avis fasse référence à la *directive sur la protection des données* (c'est-à-dire le prédécesseur ou le RGPD), de nombreux aspects sont toujours aussi applicables aujourd'hui.

Pour simplifier la détermination de la compatibilité des finalités supplémentaires, le **RGPD approuve au préalable certaines** des **finalités** supplémentaires les plus courantes poursuivies dans le cadre d'un traitement ultérieur. À savoir, l'art. 5(1)(b) comprend les éléments suivants :

> [Le traitement ultérieur à des fins d'**archivage dans l'intérêt public**, à des fins de **recherche scientifique ou historique** ou à des fins **statistiques** n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales.

L'Art. 89(1) mentionné exige la présence de garanties supplémentaires.

Dans ce cas, l'art. 89 du RGPD stipule que le traitement ultérieur à ces fins pré-approuvées n'est admissible que si des garanties adéquates sont en place.

1.2.2 Articles et considérants connexes

L'**essence** du principe de limitation de la finalité est décrite à l'**art. 5(1)(b) du** RGPD et contient également la liste des **finalités compatibles préapprouvées**.

L'art. 5(1)(e) du RGPD fournit des détails supplémentaires sur la **période de conservation** possible des données relatives à un traitement ultérieur **pour les finalités compatibles préapprouvées**.

Le considérant 50 du RGPD fournit des orientations pour l'interprétation du traitement ultérieur à des fins compatibles. La deuxième phrase, qui stipule qu'**aucune base légale supplémentaire** distincte de celle qui a permis la collecte des données à caractère personnel **n'est requise,** est particulièrement intéressante.

L'art. 89 du RGPD impose que, lorsque le traitement se poursuit à des **fins compatibles préalablement approuvées**, les responsables du traitement doivent mettre en œuvre des **garanties adéquates**. Il ouvre également la possibilité que, dans ce contexte, le droit de l'Union ou des États membres puisse prévoir des **dérogations à certains droits des personnes concernées**.

1.2.3 Mesures techniques et organisationnelles connexes

On trouvera ci-après des exemples de mesures techniques et organisationnelles à l'appui de la *limitation des objectifs* :

- Une spécification claire et précise des finalités initiales et potentiellement compatibles est une condition préalable à tout raisonnement sur la séparation des finalités.
- Il est important de comprendre la protection des données comme un processus qui comprend des **examens réguliers** tout au long du cycle de vie de l'activité de traitement pour éviter de traiter des données à des fins incompatibles, par exemple en raison d'une **dérive fonctionnelle**. Il convient de noter qu'un examen régulier est obligatoire dans le cadre de la *protection des données dès la conception* (article 25, paragraphe 1 du RGPD), des *évaluations d'impact sur la protection des données*

[84] Groupe de travail Article 29 sur la protection des données, 00569/13/FR, WP203, Avis 03/2013 sur la limitation de la finalité, adopté le 2 avril 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (dernière visite le 28/05/2020).

(article 35, paragraphe 11 du RGPD) et de la *sécurité* (article 32, paragraphe 1, point d) du RGPD).

- La **vérification de la compatibilité des finalités** conformément à l'art. 6(4) peut être considérée comme une mesure organisationnelle à l'appui de la limitation des finalités.
- **L'analyse** de la manière dont le **personnel autorisé** peut utiliser les données personnelles **à d'autres fins** est une autre mesure organisationnelle. Cette analyse vise à identifier les **motivations** et les **conflits d'intérêts** possibles (par exemple, le personnel traitant les données de parents et de connaissances), ainsi que les mesures permettant d'**éviter**[85] **ou d'atténuer** ces situations (par exemple, la possibilité pour un employé de signaler un conflit d'intérêts pour un cas donné et de le transmettre à un autre employé sans conflit d'intérêts).
- Une autre mesure consiste à analyser les **motivations que** les **attaquants externes** peuvent avoir pour obtenir les données à d'autres fins. Il s'agit d'une partie importante de l'évaluation des risques et d'une condition préalable à la mise en œuvre de mesures de protection adéquates à l'appui de la limitation de la finalité.
- Toute mesure organisationnelle ou technique visant à mettre en œuvre la **séparation entre des activités de traitement distinctes** exercées par le même responsable du traitement va directement dans le sens de la limitation de la finalité.
- Toute mesure (telle que le cryptage) en faveur de la **confidentialité** empêche les parties non autorisées d'utiliser les données à des fins illégitimes.
- Toute mesure visant à garantir que le **personnel autorisé n'**agit **que sur instruction et selon les instructions** du responsable du traitement (voir art. 29 et 32(4) du RGPD) garantit que le traitement ne va pas au-delà de ce qui est nécessaire pour réaliser les finalités spécifiques.
- **La pseudonymisation** est une mesure secondaire qui atténue les dommages après une violation. La possibilité considérablement réduite d'identifier les personnes concernées et de les relier à d'autres ensembles de données peut, dans de nombreux cas, empêcher efficacement l'utilisation des données divulguées à d'autres fins.

1.3 Minimisation des données

Bud P. Bruegger (ULD)

Remerciements : L'auteur remercie Andrès Chomczyk Penedo (VUB) qui a rédigé une analyse de ce principe comme contribution à la description présentée ici.

Les paragraphes suivants traitent du principe de *minimisation des données* qui est défini à l'art. 5(1)(c) du RGPD.

***La minimisation des données* en quelques mots :**

[85] Un autre exemple pour prévenir les conflits d'intérêts est celui d'une grande entreprise qui traite les données dans des bureaux éloignés des personnes concernées afin de réduire la probabilité que les employés traitent les données de leurs connaissances.

La minimisation des données limite les données collectées et utilisées à celles qui sont **adéquates**, **pertinentes** et **limitées** à ce qui est **nécessaire par rapport aux finalités**. La limitation au nécessaire comporte deux aspects :

- le volume des données (ou plus précisément, le contenu des informations) et
- la durée de conservation.

Par conséquent, le traitement (et la conservation) des données est réduit au minimum nécessaire, pour une durée aussi courte que possible, tout en atteignant les finalités fixées.

1.3.1 Description

Dans le document "Understanding data protection : the EU regulation in a nutshell" (Comprendre la protection des données : le règlement européen en quelques mots) ci-dessus, la *minimisation des données* était motivée par la réduction du gain de pouvoir du responsable du traitement à ce qui est minimalement nécessaire pour réaliser les finalités déclarées et légitimes. En particulier, elle vise à minimiser le contenu informatif des données personnelles traitées. Cela complète la minimisation du degré d'association des données avec la personne concernée et la limitation de l'accès au pouvoir. Voir "Minimisation du pouvoir à ce qui est nécessaire pour réaliser les finalités déclarées" pour plus de détails.

Le RGPD définit ce principe comme suit :

Définition de l'art. 5(1)(c) du RGPD :

Les données à caractère personnel doivent être **adéquates**, **pertinentes et limitées à ce qui est nécessaire au regard des finalités** pour lesquelles elles sont traitées ("*minimisation des données*") ;

Évidemment, cela n'est possible que si ces finalités sont spécifiques et explicites (comme l'exige l'art. 5(1)(b) du RGPD).

1.3.1.1 Adéquat, pertinent et limité

Adéquat et ***pertinent*** sont faciles à comprendre : Les données inadéquates, c'est-à-dire impropres aux finalités, ne peuvent être collectées ou traitées ; les données doivent également être pertinentes, c'est-à-dire qu'elles doivent servir les finalités.

Pour comprendre l'aspect de la ***limitation***, un regard plus précis sur la signification réelle des *données* est nécessaire. En particulier, il est intuitivement clair que ce n'est pas seulement le nombre d'éléments de données qui est concerné ici, mais le **contenu informatif** réel des données. Les paragraphes suivants illustrent ce point en relation avec les finalités :

- **Sélection** : Lorsqu'un ensemble d'éléments de données possibles est envisagé, il faut **sélectionner** ceux qui sont nécessaires aux fins visées. Notez que si les données sont déjà stockées, la sélection peut également être comprise comme la **suppression** d'éléments de données inutiles. Sinon, elle concerne les données qui sont effectivement collectées.
- **Résolution** : Lorsque les données sont disponibles à plusieurs résolutions possibles, **limitez la résolution** à ce qui est le moins nécessaire pour l'objectif visé. Par exemple :
    - **Valeurs** : exprimez les **valeurs** à l'**échelle la plus grossière possible** tout en respectant les objectifs,

        - par exemple, utilisez une **catégorie d'âge** (40-59 ans, résolution de 20 ans) **au lieu d'**une **date de naissance** (résolution d'un jour),
    - **Emplacements** : exprimez les **emplacements** en termes de subdivision géographique la plus grossière possible,
        - par exemple, utiliser des **unités administratives** telles que des zones de code postal ou des provinces ou encore des **cellules de grille** au lieu de coordonnées précises (d'une résolution de plusieurs mètres),
    - **Série temporelle** : exprime des **séries temporelles** de données au taux d'échantillonnage le plus grossier qui permette de réaliser les finalités fixées,
        - cela peut nécessiter un rééchantillonnage des données obtenues à partir d'un capteur,
    - **Empreintes digitales** : Si vous devez **uniquement** comparer des ensembles de données pour vérifier leur **égalité**, envisagez de traiter une certaine "**empreinte digitale**" des données.
        - Par exemple, une "valeur de hachage cryptographique" (alias "condensé") des données peut être suffisante pour détecter les modifications[86] .

- **Niveau d'agrégation** : Dans la mesure du possible, choisissez un **niveau d'agrégation** adéquat. La plupart des valeurs de données que nous traitons sont une forme d'agrégation, même si cela n'est pas évident puisqu'elle peut être effectuée de manière "invisible" par un capteur ou une méthode de collecte de données. L'agrégation est une manière de **substituer plusieurs éléments de données par un seul**. Les exemples les plus frappants proviennent des statistiques et comprennent la moyenne, la médiane, le minimum et le maximum. Dans le contexte de la protection des données, il convient de distinguer deux types d'agrégation :
    - **Personne unique** : Agrégation des éléments de données relatifs à une **seule personne** :
        - Prendre par exemple le revenu moyen d'une personne sur une année réduit le contenu de l'information relative à cette personne.
    - **Personnes multiples** : Agrégation d'éléments de données se rapportant à une **multitude de personnes** :
        - Prendre par exemple le revenu annuel moyen d'un groupe de personnes réduit également le contenu global de l'information (minimisation des données). En outre, cela affaiblit également le degré d'association entre un élément de données et une personne donnée. Ce type d'agrégation est donc également pertinent pour la limitation du stockage (voir section 1.5)

1.3.1.2 Aspect temporel

Il est clair que la minimisation des données comporte également un **aspect temporel**. Surtout, "limité à ce qui est nécessaire au regard des finalités" signifie également qu'il n'est plus justifié de conserver des données lorsque les finalités ont déjà été réalisées. Les données doivent donc être **supprimées dès qu'elles ne sont plus nécessaires**.

[86] Pour plus d'informations sur les condensés cryptographiques, voir par exemple https://en.wikipedia.org/wiki/Cryptographic_hash_function (dernière visite le 15/5/2020).

Dans la pratique, cela peut être encore **plus diversifié** : Parmi les finalités (au pluriel), certaines peuvent être réalisées plus tôt que d'autres. De même, après le "traitement principal"[87] , un "traitement ultérieur à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques"[88] peut avoir lieu. Pour modéliser cela, nous distinguons plusieurs **phases de traitement**. La figure suivante tente de visualiser cette situation.

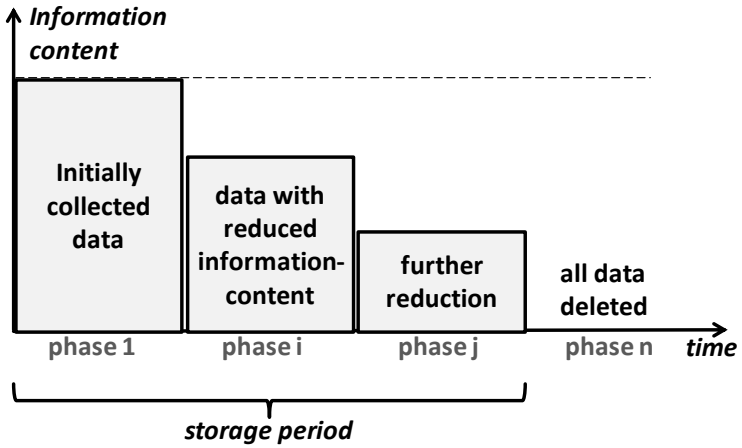

Figure 3 Réduction du contenu de l'information en plusieurs étapes.

En particulier, la figure montre un exemple avec quatre phases. Un nombre quelconque de phases est possible. Comme chaque phase est associée à un sous-ensemble de finalités, à la fin de chaque phase, lorsque les finalités respectives ont été réalisées, certaines données ne sont plus nécessaires. Par conséquent, à la **fin de chaque phase**, certaines données peuvent être **supprimées** (sélection), ou leur **contenu informatif peut être réduit** (réduction de la résolution ou augmentation du niveau d'agrégation). Il est évident qu'une telle approche diversifiée minimise davantage les données qu'une approche à phase unique qui conserve l'intégralité du contenu informatif jusqu'à ce que toutes les finalités aient été réalisées.

1.3.2 Articles et considérants connexes

Au-delà de la définition de la *minimisation des données* donnée dans l'Art. 5(1)(c), la deuxième partie de l'Art. 5(1)(e) "limitation du stockage" du RGPD stipule explicitement que :

> [Les données à caractère personnel peuvent être conservées pendant des périodes plus longues dans la mesure où les données à caractère personnel seront traitées uniquement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, sous réserve de la mise en œuvre des mesures techniques et organisationnelles appropriées requises par le présent règlement afin de sauvegarder les droits et libertés de la personne concernée ;

[87] Le terme "traitement principal" est utilisé ici pour faire la distinction avec le "traitement ultérieur".
[88] Le libellé a été directement copié de l'art. 5(1)(b) du RGPD.

Il s'agit du traitement ultérieur avec des finalités compatibles après la réalisation des finalités initiales décrites à l'art. 5(1)(b) du RGPD[89] .

Étant donné qu'il concerne le stockage des données à caractère personnel, il est considéré ici comme pertinent pour la minimisation des données puisque l'énoncé "limité à ce qui est nécessaire au regard des finalités" ne se limite pas au seul volume des données mais doit clairement être compris comme portant sur l'aspect temporel des données. En outre, la minimisation des données concerne tous les aspects du traitement (tels que la *collecte* et la *divulgation*) et s'applique donc également au *stockage*.

Pour ces raisons, la deuxième partie de l'art. 5(1)(e) du RGPD est examinée ici pour fournir des indications sur la manière d'interpréter le principe de minimisation des données dans le contexte d'un traitement ultérieur à des fins compatibles après la réalisation des finalités initiales.

Au-delà, le RGPD souligne l'importance de ce principe dans différents contextes :

Dans l'art. 25(1) du RGPD sur la ***protection des données dès la conception***, il souligne comment la ***minimisation des données*** doit être **envisagée dans chaque phase du cycle de vie** d'une activité de traitement. Cela inclut par exemple la phase d'analyse et de conception d'une activité de traitement où les objectifs du traitement sont déterminés : de toute évidence, plus les finalités sont précises et étroites, plus il devient clair quelles données sont réellement nécessaires et plus il est possible de reconnaître les données inutiles. De même, dans une phase ultérieure du cycle de vie, des mesures peuvent être prises pour mettre en œuvre la suppression ou la réduction effective du contenu des informations.

L'art. 89(1) et le considérant 156 du RGPD soulignent l'**importance de la *minimisation des données*** dans le cas où, après avoir réalisé les finalités initiales, les données sont traitées ultérieurement pour des "objectifs compatibles"[90] . En particulier, "les finalités d'**archivage** dans l'intérêt public, les finalités de **recherche scientifique** ou **historique** ou les **finalités statistiques** ne sont pas considérées comme incompatibles avec les finalités initiales"[91]conformément à l'article 89, paragraphe 1. L'art. 89(1) du RGPD (2nd phrase) impose explicitement que pour ce traitement ultérieur, "des mesures techniques et organisationnelles soient mises en place afin notamment d'assurer le respect du principe de minimisation des données ".

1.3.3 Mesures techniques et organisationnelles connexes

La liste suivante donne des exemples de mesures techniques ou organisationnelles à l'appui de la minimisation des données. Il ne s'agit pas d'une liste exhaustive, mais plutôt d'un moyen de rendre le principe plus concret :

- **Savoir quelles sont les données nécessaires aux finalités** : Savoir quelles données sont réellement nécessaires n'est possible qu'avec une définition précise et étroite des finalités. Déterminer ce qui est réellement nécessaire est une mesure de soutien à la minimisation des données qui est généralement mise en œuvre pendant la phase de conception ou de design d'une activité de traitement.

[89] En effet, l'art. 5(1)(b) contient la déclaration suivante : "un traitement ultérieur à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales, conformément à l'article 89, paragraphe 1".
[90] Voir l'art. 5(1)(b) du RGPD.
[91] Formulation tirée de l'art. 5(1)(b) du RGPD.

- **Ne recueillir que les données nécessaires** : Lors de la phase de conception et de la sélection, de la mise en œuvre et/ou de la configuration du logiciel, l'acquisition des données, par exemple au moyen de formulaires de saisie ou de boîtes de dialogue, doit être conçue de manière à ne collecter que les données nécessaires au niveau de détail requis.
- **Supprimer les données et réduire le contenu informatif entre les phases de traitement**[92]: Planifier et mettre en œuvre la fonctionnalité permettant de supprimer les données inutiles à la fin des phases de traitement ou de réduire autrement leur contenu informatif.
- **Protégez-vous contre le dépassement de la période maximale de stockage** : En deuxième ligne de défense, définissez une *durée maximale de conservation*[93] et mettez en place une procédure qui vous alerte sur la présence de données ayant dépassé cette durée. Cette mesure permet de se prémunir contre les échecs de suppression, par exemple ceux causés par un bogue logiciel qui se manifeste dans certains cas, une panne du système pendant l'opération de suppression, ou la restauration de données à partir d'une sauvegarde après une panne du système alors que les données étaient déjà supprimées auparavant.

1.4 Précision

Bud P. Bruegger (ULD)

Remerciements : L'auteur tient à remercier Frédéric Tronnier (GUF) pour sa contribution à l'analyse de ce principe, qui a servi de base à la description présentée ici.

Les paragraphes suivants traitent du principe de *précision* défini à l'art. 5(1)(d) du RGPD.

***La précision* en un coup d'œil :**

La précision des données concerne à la fois l'**exactitude factuelle** et la **mise à jour**. Il est interdit d'utiliser des données inexactes qui ne sont pas adaptées à leur finalité ou qui ont des conséquences négatives pour les personnes concernées. La principale mesure de mise en œuvre de ce principe consiste à soutenir de manière adéquate le **droit de rectification** des personnes concernées.

[92] Il convient de noter que cette déclaration est relative à l'ensemble des données détenues par le responsable du traitement. Il est également supposé ici que les données ne sont collectées qu'une seule fois auprès des personnes concernées ou à leur sujet et qu'aucune collecte ultérieure de données (par exemple, en cas de besoin) n'a lieu. La déclaration n'exclut pas que différentes phases ou étapes de traitement n'utilisent qu'un sous-ensemble des données globales.

[93] Il peut s'agir directement de "la période pendant laquelle les données à caractère personnel seront conservées" conformément à l'art. 13(2)(a) ou, si la période de conservation dépend de critères, le temps maximal pendant lequel on peut s'attendre à ce que ces conditions soient remplies.

1.4.1 Description

Dans le document "Comprendre la protection des données : le règlement européen en quelques mots" ci-dessus, la *précision* (ainsi que l'intégrité) a été motivée par le fait que la précision des données est nécessaire pour qu'elles soient adaptées aux finalités déclarées. Tout traitement qui n'est pas adapté à la finalité ne peut justifier un gain de pouvoir sur une personne concernée. Voir "Interdiction des traitements non conformes aux finalités" pour plus de détails.

Outre l'adéquation à la finalité, le traitement de données inexactes peut avoir des conséquences négatives pour les personnes concernées. Ces conséquences peuvent aller d'un effort accru nécessaire pour exercer ses droits, à la négation de droits et de possibilités, en passant par des conséquences financières ou juridiques négatives. Si l'on peut dire qu'un traitement affecté par de tels défauts n'est pas adapté à sa finalité, il violerait en outre le principe de *loyauté* (cf. **¡Error! No se encuentra el origen de la referencia.** ci-dessus).

Le RGPD définit ce principe comme suit :

Définition de l'art. 5(1)(d) du RGPD :

Les données à caractère personnel doivent être **exactes** et, si nécessaire, mises à **jour** ; **toutes les mesures raisonnables** doivent être prises pour que les **données à caractère personnel qui sont inexactes**, eu égard aux finalités pour lesquelles elles sont traitées, soient **effacées ou rectifiées** sans délai (*"précision")* ;

Les paragraphes suivants traitent plus en détail des différents aspects de la *précision* :

1.4.1.1 Comment évaluer la précision ?

Le concept de précision doit être objectif. Il doit être possible de vérifier sans aucune ambiguïté si les données sont exactes ou non, et différents vérificateurs doivent parvenir à la même évaluation. Cela n'est possible que lorsque les données représentent des **faits vérifiables**. Ce n'est par exemple pas le cas pour les données qui représentent une expression ou l'opinion d'une personne.

La vérification de la précision des données implique donc généralement la vérification des faits qui sous-tendent les données. Par exemple, pour vérifier qu'un numéro de téléphone mobile appartient bien à une personne, on peut envoyer et recevoir un message test avec un code aléatoire sur un autre canal.

Dans certaines situations, il se peut que ce soit la personne concernée qui fournisse au responsable du traitement la documentation nécessaire sur les faits permettant une vérification. Par exemple, une personne concernée peut fournir un certificat de résidence délivré par une autorité de confiance afin d'étayer la vérification d'une adresse de résidence.

1.4.1.2 Que signifie "à jour" ?

Pour déterminer si les données sont à jour, il faut tenir compte des finalités du traitement. Par exemple, un vendeur peut stocker l'adresse de livraison d'une personne concernée alors que celle-ci a depuis déménagé dans une nouvelle résidence. Si la finalité du traitement est de livrer effectivement des marchandises à la personne concernée, l'adresse est manifestement périmée et les données sont inadaptées à la finalité. En revanche, si la finalité du traitement est la facturation des marchandises déjà livrées, l'ancienne adresse doit être considérée comme actuelle.

1.4.1.3 Comment l'inexactitude des données est-elle découverte ?

Les données inexactes (y compris les données périmées) doivent être rectifiées ou supprimées par le responsable du traitement sans délai. Mais comment l'inexactitude des données est-elle effectivement découverte et quelles sont les implications pour les responsables du traitement ?

Le mécanisme probablement le plus important permettant aux responsables du traitement de détecter l'inexactitude de leurs données est la **notification par la personne concernée**[94] . En particulier, la personne concernée doit avoir connaissance du traitement (voir les articles 13 et 14 du RGPD) et peut accéder aux données utilisées par le responsable du traitement (voir l'article 15 du RGPD). Sur cette base, elles peuvent vérifier la précision de leurs données et, si nécessaire, invoquer leur **droit de** demander la **rectification** de leurs données (voir art. 16 du RGPD). Dans ce cas, un responsable du traitement remplit l'obligation de vérifier la précision en soutenant de manière adéquate le droit de rectification dans son traitement.

Lorsque les données sont collectées directement auprès des personnes concernées, il est plus raisonnable pour un responsable du traitement de supposer que les données obtenues sont exactes (au moins au moment de la collecte). La situation peut être différente lorsque les données sont collectées auprès d'une autre source. Dans ce cas, le responsable du traitement a l'obligation de vérifier la précision des données obtenues, au moins en ce qui concerne leur adéquation aux finalités déclarées du traitement et les conséquences négatives que des inexactitudes peuvent avoir pour les personnes concernées.

Pour certains éléments de données, le fait qu'ils aient été directement collectés auprès des personnes concernées peut ne pas être suffisant pour qu'un responsable du traitement présume de leur précision. C'est le cas lorsqu'une demande potentiellement inexacte entraîne des avantages pour la personne concernée. Dans ces cas, le responsable du traitement peut avoir besoin de procéder à une vérification des données en amont, en tant que partie intégrante de la collecte des données. Cela est possible, par exemple, en demandant aux personnes concernées de fournir une certification des faits revendiqués par une autorité de confiance.

1.4.2 Articles et considérants connexes

L'article du RGPD le plus étroitement lié au principe de *précision* est le ***droit de rectification***. Sa pertinence a déjà été examinée dans la section 1.4.1.3 ci-dessus. Des **informations** adéquates permettant aux personnes concernées de prendre conscience du traitement (**articles 13 et 14 du RGPD**) et le **droit d'accéder** aux données en possession du responsable du traitement (**article 15**) peuvent être considérées comme nécessaires pour permettre le droit de rectification.

Lorsqu'un responsable du traitement ne peut pas donner suite instantanément à une demande de rectification (selon l'art. 16 du RGPD), mais a besoin d'un délai suffisant pour vérifier la précision des données en question, il peut être nécessaire de **limiter le traitement** des données (voir **art. 18(1)(a)** du RGPD). Après la vérification de la précision et la rectification effectuée, le responsable du traitement doit **informer la personne concernée** conformément à l'**art. 12(3)** du RGPD. Si le responsable du traitement constate que les données sont effectivement exactes et ne nécessitent pas de rectification, la **personne concernée** doit être **informée conformément** à l'**art. 12(4)** du RGPD. Si le traitement était limité, la personne concernée peut alors **consentir à la levée de la limitation**, même sans rectification (voir l'**art. 18(2)** du RGPD). En l'absence d'un tel consentement, le responsable du traitement peut soit

[94] D'autres mécanismes comprennent par exemple des contrôles de cohérence, une variance excessive ou un manque de corrélation attendue.

effacer les données (voir l'**art. 5(1)(d)** du RGPD) ou demander à son délégué à la protection des données de **consulter l'autorité de contrôle** sur la question (voir **art. 39(1)(e)** du RGPD).

Dans le cas où le responsable du traitement a communiqué les données à des **destinataires**, ceux-ci **doivent également être informés** de l'inexactitude (conformément à l'**article 19** du RGPD). En particulier, les responsables du traitement sont tenus de notifier aux destinataires les rectifications qui ont été effectuées. Étant donné que la vérification de la précision peut dépendre des finalités du traitement (cf. 1.4.1.2 ci-dessus), il peut être utile et plus opportun de déjà notifier volontairement aux destinataires la demande de rectification. Cette approche étendue couvre également le cas où les données sont exactes pour le responsable du traitement, mais nécessitent une rectification chez l'un des destinataires.

Les **personnes concernées** ont également le **droit de demander à être informées de ces notifications** (voir la deuxième phrase de l'**article 19** du RGPD). Ces informations comprennent la désignation des destinataires individuels[95] .

1.4.3 Mesures techniques et organisationnelles connexes

Toute organisation ou mesure technique visant à faciliter la détection des inexactitudes ou la rectification (ou la suppression) des données en temps utile soutient le principe de *précision*. Pour comprendre quand la précision est particulièrement importante et quand des mesures plus strictes sont nécessaires, il faut analyser comment les inexactitudes sont liées à l'aptitude à l'emploi et comment elles peuvent nuire aux personnes concernées.

Voici quelques exemples de mesures possibles à l'appui de la précision :

- une mesure organisationnelle au moment de la conception est l'analyse du niveau minimal de précision requis pour être adapté à l'objectif ;
- une mesure organisationnelle au moment de la conception est l'analyse des éventuels impacts négatifs que des données inexactes peuvent avoir sur les personnes concernées ;
- une mesure du temps de conception est l'analyse de la précision des données obtenues à partir de sources autres que les personnes concernées elles-mêmes ;
- une autre est l'analyse de la nécessité de vérifier certains éléments de données au préalable (voir 1.4.1.3 ci-dessus) ;
- une autre mesure de conception consiste à formuler des exigences pour le soutien des droits à l'information (article 13 ou 14 du RGPD), le droit d'accès (article 15 du RGPD) et, surtout, le droit de rectification (article 16 du RGPD) ;
- il en va de même pour la mise en œuvre des notifications des destinataires (art. 19 du RGPD) concernant l'inexactitude et la rectification ;
- au moment de la mise en œuvre de l'activité de traitement, la désignation du personnel pour une éventuelle intervention manuelle nécessaire pour vérifier la précision ou effectuer une rectification est une mesure d'organisation possible ;
- il en va de même pour préparer le délégué à la protection des données à traiter efficacement les demandes de rectification.

[95] Ceci est intéressant puisque dans les art. 13(1)(e) et 14(1)(e), il suffit d'informer sur les catégories de destinataires.

1.5 Limitation du stockage

Bud P. Bruegger (ULD)

Les paragraphes suivants traitent du principe de la *limitation du stockage* qui est défini à l'art. 5(1)(e) du RGPD.

***La limitation du stockage* en quelques mots :**

La limitation du stockage (même si son nom ne l'implique pas) tient compte du degré d'**identification des** personnes concernées par les données, c'est-à-dire de la facilité avec laquelle la personne concernée peut être associée aux données. Les degrés d'identification prévus par le RGPD sont les ***données d'identification directe*** qui contiennent des *identifiants*, les ***données pseudonymes*** et les ***données anonymes***. Les données doivent être collectées avec le plus faible degré d'identification possible et la pseudonymisation et l'anonymisation doivent être utilisées pour réduire davantage l'identification dès que possible au fil du temps.

1.5.1 Description

Dans le document "Comprendre la protection des données : le règlement européen en quelques mots" ci-dessus, la *limitation du stockage* était motivée par la réduction du gain de pouvoir du responsable du traitement à ce qui est minimalement nécessaire pour réaliser les finalités déclarées et légitimes. En particulier, elle vise à réduire au minimum le degré d'association des données à caractère personnel avec la personne concernée. Cela complète la minimisation du contenu de l'information et la limitation de l'accès au pouvoir. Voir "Minimisation du pouvoir à ce qui est nécessaire pour réaliser les finalité déclarées" pour plus de détails.

Le RGPD définit ce principe comme suit :

Définition de l'art. 5(1)(e) du RGPD :

Les données à caractère personnel sont **conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités** pour lesquelles elles sont traitées ; [...] ("*limitation du stockage*") ;

Il est clair que le concept principal de ce principe concerne l'***identification***, c'est-à-dire l'association des données personnelles à la personne concernée. Le reste de cette section analyse donc principalement ce que signifie réellement l'identification.

Notez que dans l'encadré de définition ci-dessus, la partie omise qui est représentée par [...] a été discutée sous le principe de la *minimisation des données* (voir section 1.3.2 "Articles et considérants connexes" dans "Minimisation des données"). Elle concerne la **limitation temporelle du stockage** qui est sans doute un aspect du **concept** général **de limitation** exprimé pour les données dans le principe de *minimisation des données.*

De ce point de vue, l'appellation "*limitation du stockage"* est trompeuse car elle implique uniquement l'aspect temporel de la minimisation des données et ne fait pas référence à

l'identification dans son ensemble. Il serait peut-être plus clair de parler de *minimisation du potentiel d'identification*.

1.5.1.1 Identification des personnes concernées

Pour mieux comprendre ce que l'on entend par identification, nous nous référons à l'art. 4(1) du RGPD. La deuxième demi-phrase[96] se lit comme suit :

> [Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique ;

Pour une meilleure compréhension, cette phrase est divisée en deux parties :

Identification directe par référence à un identifiant :

> [Une personne physique identifiable est une personne qui peut être identifiée, **directement** ~~ou indirectement~~, notamment par référence à un **identifiant** tel qu'un *nom*, un *numéro d'identification*, des *données de localisation*, un *identifiant en ligne* ~~ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique~~ ;

Identification indirecte par référence à un ou plusieurs facteurs spécifiques à l'identité d'une personne physique :

> [Une personne physique identifiable est une personne qui peut être identifiée, ~~directement ou~~ **indirectement**, notamment par référence ~~à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou~~ à **un ou plusieurs facteurs spécifiques à l'identité** *physique*, *physiologique*, *génétique*, *mentale*, *économique*, *culturelle* ou *sociale* **de cette personne physique** ;

Les **exemples d'identifiants** sont[97] :

- Un nom,
- un numéro d'identification,
- les données de localisation,
- un identifiant en ligne.

Il convient de noter en particulier les *données de localisation* qui ne sont peut-être pas considérées comme un identifiant permettant une identification directe, même si leur caractère hautement identifiant est effectivement intuitif.

Les exemples de **facteurs spécifiques à l'identité d'une personne physique** concernent les aspects suivants :

- Physique,
- physiologique,
- génétique,

[96] Une partie de phrase séparée du reste par un point-virgule est appelée ici "demi-phrase".

[97] Notez que le considérant 30 du RGPD fournit en outre des exemples d'"identifiants en ligne" : adresses de protocole internet, identifiants de cookies ou autres identifiants tels que les étiquettes d'identification par radiofréquence.

- mental,
- économique,
- culturel,
- sociale.

Cette distinction de l'identification directe et indirecte permet désormais de diversifier la notion de *formulaire permettant l'identification des personnes concernées*.

1.5.1.2 Types de données distingués dans le RGPD

Le RGPD distingue trois types de données avec différents degrés d'association avec les personnes concernées :

(i) **les données personnelles directement identifiantes**[98] ,

(ii) **les données personnelles pseudonymes**, et

(iii) **les données anonymes**.

(i) Données personnelles directement identifiantes : Le premier élément doit évidemment contenir des **identifiants**, puisqu'il permet l'identification directe des personnes concernées. La plupart des ensembles de données à caractère personnel ne contiennent cependant pas que des identifiants. Il faut alors considérer que les autres données sont toutes des **éléments propres à l'identité d'une personne physique** puisqu'elles décrivent toutes différents aspects liés à l'identité de la personne concernée.

(ii) Données personnelles pseudonymes : L'art. 4(5) du RGPD définit le concept connexe de "pseudonymisation". Son libellé peut être adapté comme suit pour définir les données personnelles pseudonymes :

> Les données personnelles pseudonymes sont des données personnelles qui **ne peuvent plus être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires**.

Ceci doit être interprété de la manière suivante :

- Les données personnelles pseudonymes **ne permettent pas une identification directe**.
- Elles **ne doivent** donc **pas contenir d'identifiants**.
- **Les données supplémentaires**, dans ce contexte, sont des données qui permettent d'**associer des facteurs spécifiques à l'identité d'une personne physique à des identifiants.**

(iii) Données anonymes : Les informations anonymes sont définies au considérant 26 du RGPD (cinquième phrase). En utilisant l'*information* et les *données* comme synonymes, son libellé peut être adapté comme suit :

> Les données anonymes sont soit
>
> - des données qui ne concernent pas une personne physique identifiée ou identifiable ou

[98] Le terme "*données personnelles directement identifiantes*" n'est pas utilisé dans le RGPD mais cloné par l'auteur.

- des données personnelles rendues anonymes de telle sorte que la personne concernée ne soit pas ou plus identifiable.

Notez que le terme "identifiable" recouvre à la fois l'identification directe et indirecte. Même avec des informations supplémentaires, il n'est pas possible d'attribuer des données anonymes à une personne spécifique.

Notez que selon le considérant 26 (phrase 6), le RGPD ne s'applique pas aux données anonymes. Cela est également clair puisqu'elles ne correspondent pas à la définition des données à caractère personnel (voir art. 4(1) et le considérant 26 du RGPD).

Après avoir distingué ces types de données, "conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités" peut maintenant être compris de manière plus précise, en considérant également l'aspect temporel du principe.

1.5.1.3 Aspect temporel

L'art. 5(1)(e) aborde clairement l'aspect temporel en stipulant qu'un formulaire permettant l'identification doit être conservé **pendant une durée n'excédant pas** celle nécessaire à la réalisation des finalités. Cet aspect temporel est abordé ici de manière diversifiée. Les deux critères suivants définissent cette diversification :

- **L'identification** peut être **directe** ou **indirecte**.
- **L'identification** peut être **accessible à tous** ou à **un groupe restreint de personnes.**

Sur la base de ces distinctions, il est possible de distinguer quatre cas différents. Ceux-ci sont Figure 1 représentés comme des "phases". Il est possible de passer d'une phase à n'importe quelle phase ultérieure. Cela peut se faire soit de manière séquentielle, soit en omettant les phases intermédiaires. Dans chaque phase, le degré d'identification des données avec la personne concernée est réduit. Le principe de *limitation du stockage* stipule qu'à tout moment, seul **le degré minimal d'identification nécessaire à la réalisation des finalités doit être utilisé**.

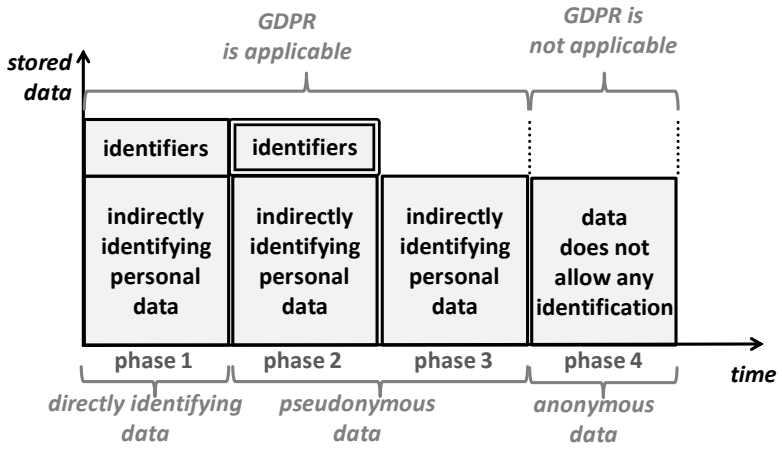

Figure 1: Données avec différents degrés d'association avec la personne concernée.

Il convient de noter que le principe de la *limitation du stockage* est présenté dans sa forme pure : le degré d'association avec la personne concernée est purement réduit entre deux phases consécutives. Dans la pratique, la limitation du stockage est généralement combinée avec la

minimisation des données. Dans un scénario combiné, la hauteur des cases illustrées dans la figure serait également réduite.

Les phases de la figure sont décrites plus en détail dans ce qui suit :

La phase 1 montre les données qui contiennent à la fois des **identifiants** et des **facteurs spécifiques à l'identité d'une personne physique**. Par souci de concision, ces dernières sont appelées *données personnelles directement identifiantes*. Les identifiants permettent une identification directe. Elles sont **accessibles** à **toute personne à qui les données sont divulguées**.

La **phase 2** présente un mode de traitement appelé "**pseudonymisation**"[99] . Dans ce cas, les **identifiants** sont toujours stockés, mais ils sont **conservés séparément** et **protégés** de manière à ce que l'**accès ne soit** possible **que** dans des **conditions bien définies,** selon des **procédures prédéfinies**, pour réaliser des **finalités précisément définies**, l'accès étant limité à un **ensemble prédéfini de personnes autorisées**[100] . Ces restrictions sont représentées par une double bordure autour des identifiants. L'**accès à l'identification directe** est donc **étroitement contrôlé** et n'est accessible qu'à quelques personnes désignées.

L'identification indirecte qui utilise des informations supplémentaires est toujours possible sur la base des données personnelles indirectement identifiantes. Elle nécessite toutefois des informations supplémentaires. Le responsable du traitement met en œuvre des mesures pour empêcher la disponibilité de ces informations supplémentaires pour les personnes qui accèdent à ces données pendant l'activité de traitement. Cela signifie que **pour la grande partie du traitement** (et un sous-ensemble important de finalités), et pour la majorité des employés, l'**identification n'est plus possible**.

La phase 3 montre la situation dans laquelle les **finalités ne nécessitent plus la possibilité d'une identification directe** des personnes concernées, même pas dans des cas exceptionnels. Dans ce cas, les *identifiants* qui permettent une identification directe peuvent être purement et simplement supprimés. Par conséquent, si des mesures de protection adéquates sont en place, **le responsable du traitement lui-même** (y compris l'ensemble du personnel) **n'est plus en mesure d'identifier les personnes concernées**. De toute évidence, cela réduit encore le degré d'identification par rapport à la phase 2.

La phase 4 montre que seules des **données anonymes** sont utilisées. Ce chiffre implique que celles-ci sont le résultat d'une anonymisation des données de la phase 3 (ou des phases précédentes). Par définition[101] , les données anonymes ne peuvent pas être attribuées à une personne concernée, même en utilisant des informations supplémentaires. Ces données ne sont donc plus des données à caractère personnel et ne sont donc pas soumises au RGPD (et une anonymisation réussie a donc le même effet qu'une suppression). Les **données anonymes éliminent donc complètement la possibilité d'identification**.

Certains lecteurs connaissent peut-être le concept de "***non-liaison***"[102] , qui est étroitement lié à celui de limitation de stockage. Cela devient clair si l'on considère que l'identification directe peut être considérée comme un identifiant établissant un lien avec la personne concernée ; et que l'utilisation d'informations supplémentaires pour l'identification indirecte nécessite de relier les enregistrements de données qui appartiennent à la même personne dans les deux ensembles de données.

---

[99] Voir l'article 4, paragraphe 5, du RGPD.

[100] Voir le considérant 29 du RGPD, 2nd phrase.

[101] Voir le considérant 26 du RGPD.

[102] Conférence allemande des autorités indépendantes de protection des données de la Fédération et des Länder, 17 avril 2020. Le modèle standard de protection des données, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b_EN.pdf (dernière visite le 28/05/2020).

1.5.2 **Articles et considérants connexes**

Comme cela a été montré, plusieurs concepts définis en dehors de l'Art 5 du RGPD sont pertinents pour la compréhension du principe de limitation de stockage. Il s'agit en particulier de :

- *Identification directe* et *indirecte* définie à l'art. 4(1) du RGPD,
- *la pseudonymisation* qui est définie à l'art. 4(5) du RGPD, et
- *les données anonymes* définies au considérant 26 du RGPD.

Dans l'art. 11(1), le RGPD stipule :

> Si les finalités pour lesquelles un responsable du traitement traite des données à caractère personnel ne nécessitent pas ou plus l'identification d'une personne concernée par le responsable du traitement, ce dernier n'est pas tenu de conserver, d'acquérir ou de traiter des informations supplémentaires afin d'identifier la personne concernée dans le seul but de se conformer au présent règlement.

Cela donne des indications sur l'importance que revêt le principe de limitation du stockage par rapport à d'autres concepts du RGPD: la limitation du stockage a une nette préséance sur les autres obligations du RGPD en ce sens qu'un responsables du traitement ne doit pas collecter ou stocker des identifiants dans le seul but de se conformer à ces obligations.

L'article 11, paragraphe 2, du RGPD[103] le stipule explicitement pour les obligations relatives aux droits des personnes concernées visés aux articles 15 à 20 :

> Lorsque, dans les cas visés au paragraphe 1 du présent article, les responsables du traitement sont en mesure de démontrer qu'ils ne peuvent pas identifier la personne concernée, ils en informent la personne concernée, si possible. Dans ces cas, les articles 15 à 20 ne s'appliquent pas, sauf si les personnes concernées, aux fins de l'exercice des droits que leur confèrent ces articles, fournissent des informations supplémentaires permettant leur identification.

En outre, le RGPD souligne l'importance de la pseudonymisation dans divers contextes :

L'art. 89(1) souligne l'**importance de la *pseudonymisation*** dans le cas où, après la réalisation des finalités initiales, les données sont traitées ultérieurement pour des "finalités compatibles"[104] . En particulier, "les finalités d'**archivage** dans l'intérêt public, les finalités de **recherche scientifique** ou **historique** ou les **finalités statistiques** ne sont pas considérées, conformément à l'article 89, paragraphe 1, comme incompatibles avec les finalités initiales"[105] . L'art. 89(1) du RGPD (2nd phrase) stipule explicitement que pour ce traitement ultérieur, "des mesures techniques et organisationnelles doivent être mises en place et cite la pseudonymisation comme seul exemple de telles mesures (3rd phrase). Elle indique en outre (4th phrase) : "Lorsque ces finalités peuvent être réalisées par un traitement ultérieur qui ne permet pas ou plus l'identification des personnes concernées, ces finalités sont réalisées de cette manière." Il semble s'agir d'une application directe du principe de limitation du stockage.

L'art. 6(4)(e) souligne en outre le rôle de la pseudonymisation lorsqu'un responsable du traitement détermine si une finalité supplémentaire est compatible avec les finalités pour lesquelles les données ont été collectées.

---

[103] Voir également l'art. 12(2) du RGPD qui traite plus en détail de ce cas.
[104] Voir l'art. 5(1)(b) du RGPD.
[105] Formulation tirée de l'art. 5(1)(b) du RGPD.

L'art. 25(1) énumère la pseudonymisation comme seul exemple de mesure pouvant être mise en œuvre lors de la protection des données par conception.

L'art. 32(1)(a) énumère le pseudonymisation avec le cryptage comme une mesure de soutien à la sécurité. Si cela souligne encore l'importance de la pseudonymisation et donc de la limitation du stockage, on peut toutefois se demander si la pseudonymisation soutient effectivement l'un des objectifs de protection communs de la sécurité informatique, à savoir la *confidentialité*, l'*intégrité* et la *disponibilité*.

1.5.3 Mesures techniques et organisationnelles connexes

Voici quelques exemples de mesures concrètes qui soutiennent le principe de la limitation du stockage :

- Au moment de la conception d'une activité de traitement donnée, une mesure organisationnelle consiste à **vérifier si des données personnelles directement identifiantes doivent être collectées** pour réaliser les finalités fixées.
- **La pseudonymisation** et l'**anonymisation** des données entre les étapes du traitement sont des mesures techniques primordiales. Elles nécessitent de vérifier si les finalités restantes après l'achèvement de l'étape de traitement nécessitent toujours le même degré d'identification des personnes concernées.
- Lorsqu'il est prévu de délivrer des identifiants d'authentification aux personnes concernées, une mesure organisationnelle consiste à vérifier s'il est suffisant de **délivrer des identifiants pseudonymes**. Par exemple, l'attribution d'un mot de passe aléatoire à usage unique pendant la collecte des données peut suffire à justifier ultérieurement le droit de retirer le consentement.
- Concevoir un site web de manière à ce qu'il **s'abstienne d'installer des cookies en** dehors des zones nécessitant une authentification **permet d'éviter un moyen d'identifier les personnes concernées** d'une session à l'autre et peut être considéré comme une mesure de soutien à la limitation du stockage (voir "Configuration des cookies et rédaction d'une politique en matière de cookies"). Concrètement, cela peut se faire via une configuration appropriée de l'application web (comme un système de gestion de contenu et ses plugins) ou du serveur web.
- Le fait d'exploiter un service basé sur l'internet de manière à **permettre aux** utilisateurs de se connecter via un **réseau superposé anonyme tel que TOR**[106] évite d'identifier les personnes concernées par leur adresse IP (réseau) et constitue donc une mesure en faveur de la limitation du stockage.
- Equiper un **dispositif utilisateur compatible Wi-Fi** d'une **randomisation d'adresse MAC**[107] de manière à empêcher la personne concernée de diffuser des identifiants uniques.

1.6 Intégrité et confidentialité

Bud P. Bruegger (ULD)

[106] Voir par exemple, https://en.wikipedia.org/wiki/Tor_(anonymity_network) (dernière visite le 18/5/2020).
[107] Voir, par exemple, https://en.wikipedia.org/wiki/MAC_spoofing#MAC_Address_Randomization_in_WiFi (dernier accès le 18/5/2020).

Remerciements : L'auteur tient à remercier Frédéric Tronnier (GUF) pour sa contribution à l'analyse de ce principe, qui a servi de base à la description présentée ici.

Les paragraphes suivants traitent du principe d'*intégrité et de confidentialité* qui est défini à l'art. 5(1)(f) du RGPD.

***Intégrité et confidentialité* en quelques mots :**

Ce principe fait référence aux objectifs classiques de protection de la **sécurité** informatique, à savoir la ***confidentialité***, l'***intégrité*** et la ***disponibilité*** (CIA). La ***résilience*** peut être considérée comme un aspect de la disponibilité. L'objectif principal est de protéger le patrimoine contre les *risques* causés par des *événements indésirables*. Contrairement à la sécurité informatique, ce **patrimoine et ces risques** ne sont pas ceux du responsable du traitement (une organisation), mais ceux **des personnes concernées**. De ce point de vue, la raison pour laquelle la *portabilité des données* s'inscrit dans la *disponibilité* au sein de ce principe est également claire : elle protège les personnes concernées de la perte d'un actif (représenté par les données) lorsqu'elles changent de responsable des données (le plus souvent de fournisseur).

1.6.1 Description

Dans le document "Comprendre la protection des données : le règlement européen en quelques mots" ci-dessus, l'*intégrité* (ainsi que la précision) a été motivée par le fait que la précision des données est nécessaire pour qu'elles soient adaptées aux finalités déclarées. Tout traitement qui n'est pas adapté à la finalité ne peut justifier un gain de pouvoir sur une personne concernée. Voir "Interdiction des traitements non adaptés aux finalités" pour plus de détails. En revanche, la *confidentialité* a été motivée par la limitation de l'accès au pouvoir. Voir la section 1.6.5.3 "Limitation de l'accès au pouvoir" pour plus de détails. La *disponibilité* était motivée par la protection du patrimoine de la personne concernée. Voir section "1.6.6. Protection du patrimoine de la personne concernée" pour plus de détails.

Le RGPD définit ce principe comme suit :

Définition de l'art. 5(1)(f) du RGPD :

Les données à caractère personnel sont traitées d'une manière qui **garantit une sécurité appropriée** des données à caractère personnel, y compris la protection contre le **traitement non autorisé** ou **illégal** et contre la **perte, la destruction** ou les **dommages accidentels**, au moyen de mesures techniques ou organisationnelles appropriées ("*intégrité et confidentialité*").

1.6.1.1 La structure de l'art. 5(1)(f) et les risques de sécurité

Ce qui ressort de la formulation de l'art. 5(1)(f) est que le RGPD parle d'**événements non désirés**, à savoir :

- le traitement non autorisé ou illégal, et
- la perte, la destruction ou les dommages accidentels.

Il est clair que ces événements ne font pas partie du traitement prévu ; l'idéal serait de les éviter complètement. Étant donné qu'en matière de sécurité, cela n'est jamais possible avec une certitude de 100%, il existe une **probabilité** résiduelle **que de tels événements se produisent**.

Il est également évident que l'apparition de tels événements a des **conséquences indésirables**.

Les lecteurs familiers de la sécurité informatique auront reconnu que cette discussion a introduit les éléments utilisés dans la définition du *risque*. Ceci est rendu explicite dans ce qui suit :

Risque de sécurité = probabilité d'un événement indésirable * gravité des conséquences indésirables

Il s'agit d'un risque "individuel" et le risque total est alors la somme de tous les risques individuels applicables.

Les lecteurs attentifs auront peut-être remarqué que la terminologie utilisée ici diffère quelque peu de celle qui est couramment employée dans le domaine de la sécurité informatique[108] . En particulier, le terme "risque de sécurité" a été utilisé, plutôt que le simple "risque", et de même, "gravité des conséquences indésirables" a été utilisé au lieu de "dommages". La motivation de ce choix de termes est expliquée dans ce qui suit :

1.6.1.2 Principale différence par rapport aux autres risques du RGPD et aux risques en matière de sécurité informatique

Le RGPD fait référence à au moins deux types de risques fondamentalement différents (mais sans rendre cette distinction explicite). Les paragraphes suivants introduisent donc deux termes différents pour rendre cette distinction explicite. Il s'agit du *risque lié à la sécurité* et du *risque lié à la protection des données*.

Dans le RGPD, le ***risque de sécurité*** est implicite dans les articles 5(1)(f) et 32. Comme il ressort de la sous-section précédente, sa définition découle de l'existence d'**événements indésirables** qui **ne font pas partie des opérations de traitement prévues**.

En revanche, le RGPD prend clairement en compte les risques découlant du traitement des données lui-même - en l'absence de tout événement indésirable - c'est-à-dire lors d'un traitement non perturbé comme prévu. Nous appelons ce type de risque le *risque lié à la protection des données.* Il est présent, même si la sécurité était parfaite et que tous les événements indésirables possibles pouvaient être évités avec une certitude de 100 %.

Il est donc important de comprendre que les *risques de sécurité* ne sont qu'un sous-ensemble des risques que les responsables du traitement sont tenus d'atténuer par la mise en œuvre de mesures techniques et organisationnelles appropriées.

Après avoir distingué les risques de sécurité des risques de protection des données, comparons les risques de sécurité du RGPD avec ceux de la sécurité informatique. Puisque sa définition fournie dans l'encadré de la sous-section précédente a la même structure, peut-on conclure que les *risques de sécurité* du RGPD sont les mêmes que ceux de la sécurité informatique ?

Cela met en évidence le choix du second terme, à savoir la *gravité des conséquences indésirables* au lieu des *dommages*.

En matière de **sécurité informatique**, le ***dommage*** est une quantification des conséquences indésirables par rapport à la **mission et aux valeurs de l'organisation** qui exploite l'activité

[108] Voir par exemple https://en.wikipedia.org/wiki/IT_risk#Measuring_IT_risk (dernière visite le 19/05/2020).

de traitement. Il est souvent quantifié en termes de **valeur monétaire**, ce qui **correspond à** une organisation dont la mission est de produire des **bénéfices**.

En revanche, la **gravité des conséquences indésirables** inhérentes au principe d'intégrité et de confidentialité **du RGPD** contraste fortement avec cette situation**.** Cette mesure **fait référence** aux **droits et libertés des personnes physiques** tels qu'ils sont énoncés dans la Charte européenne des droits fondamentaux. L'effet indésirable peut donc consister à entraver ou à nier le libre exercice des droits et libertés d'une personne[109] . Ces effets ne peuvent généralement pas être mesurés en termes de valeurs monétaires. Il est aussi généralement impossible de les quantifier, et ils ne peuvent être exprimés que sur une échelle de mesure ordinale (par exemple celle composée de *faible*, *moyen* et *élevé*).

Ainsi, la **différence** entre la **sécurité informatique** et la **sécurité au sens de l'art. 5(1)(f)** du RGPD est l'**évaluation des conséquences indésirables**, même si les événements indésirables peuvent être les mêmes. Dans de nombreux cas, un événement qui n'a que des conséquences mineures sur la mission de l'organisation du responsable du traitement peut porter gravement atteinte aux droits et libertés d'une personne concernée (et vice versa).

1.6.1.3 Les objectifs de protection inhérents à l'art. 5(1)(f)

Le RGPD nomme ce principe défini à l'art. 5(1)(f) uniquement ***intégrité*** *et* ***confidentialité***. Il s'agit de deux des trois objectifs de protection bien connus de la sécurité informatique. Le troisième est la ***disponibilité***. Cette triade d'objectifs de protection est souvent désignée par l'acronyme *CIA*.

Alors que le nom du principe donné dans le RGPD semble suggérer que la disponibilité est exclue, tant le libellé exact de l'art. 5(1)(f) et de l'art. 32 "Sécurité du traitement" suggèrent le contraire. En particulier :

- la mention "protection contre les pertes accidentelles" peut être clairement associée à la *disponibilité*, et
- l'art. 32(1)(b) donne mandat aux responsables du traitement de "garantir en permanence la *confidentialité*, l'*intégrité*, la *disponibilité* et la ***résilience*** des systèmes et services de traitement".

La résilience est désignée ici comme le quatrième objectif de protection. Elle est aussi clairement acceptée comme un objectif de la sécurité informatique, souvent traitée comme un aspect de la *disponibilité*.

En conclusion, l'art. 5(1)(f) du

RGPD fait référence à l'ensemble des objectifs de protection connus de la sécurité informatique. Ils seront tous abordés ici sans restreindre la discussion aux deux seuls qui font partie du nom du principe.

Pour une discussion approfondie, voir les publications de l'ENISA sur le sujet[110] ,[111] . Ce qui suit ne donne qu'une brève description de chaque objectif de protection.

---

[109]Felix Bieker, Benjamin Bremert, Identifizierung von Risiken für die Grundrechte von Individuen, in : ZD, 2020, p. 7 et suivantes. (en allemand, résumé en anglais).

[110] ENISA, Lignes directrices pour les PME sur la sécurité du traitement des données personnelles, 27 janvier 2017, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing (dernière visite le 19/05/2020).

[111]ENISA, Handbook on Security of Personal Data Processing, 29 janvier 2018, https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing (dernière visite le 19/05/2020).

1.6.1.4 Intégrité

L'intégrité fait référence à l'aspect de l'art. 5, paragraphe 1, point f), qui exige la protection des données à caractère personnel "contre les dommages accidentels", par exemple en raison d'une erreur de transmission. Elle vise donc à prévenir tout type d'événement susceptible de "corrompre" les données d'une manière qui les rende impropres aux finalités du traitement.

1.6.1.5 Confidentialité

La confidentialité fait référence à l'aspect de l'art. 5(1)(f) qui exige la protection des données à caractère personnel "contre tout traitement non autorisé ou illicite". Il est important de noter que dans le RGPD, le *traitement* englobe également la *divulgation* des données (voir l'article 4(2) du RGPD). La confidentialité exige donc de protéger les données à caractère personnel contre toute divulgation indésirable lorsqu'elles sont au repos, en transit et en cours d'utilisation[112] . En outre, elle exige qu'aucune personne non autorisée ne puisse interagir avec le traitement, par exemple en introduisant des décisions qui concernent une personne, en modifiant ou en supprimant des données à caractère personnel, ou en déclenchant toute autre opération réservée au personnel autorisé qui travaille selon des instructions précises du responsable du traitement.

1.6.1.6 Disponibilité, résilience et portabilité

La disponibilité fait référence à l'aspect de l'art. 5(1)(f) qui exige la protection des données à caractère personnel "contre la perte ou la destruction accidentelle", par exemple en raison de la défaillance d'un composant de stockage.

La résilience semble être définie à l'art. 32(1)(c) comme "la capacité de rétablir la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique". Il s'agit donc clairement d'un aspect de la disponibilité et elle est liée à la mesure bien connue de la reprise après sinistre.

On peut soutenir qu'un autre aspect de la *disponibilité* est la *portabilité* des données telle qu'elle est définie à l'art. 20 du RGPD. Alors que la disponibilité est généralement comprise comme la protection des personnes concernées contre la perte de leurs données lorsqu'elles sont traitées par un responsable du traitement donné, la *portabilité des* données protège les personnes concernées contre la perte lorsqu'elles passent d'un responsable du traitement (par exemple, en tant que prestataire de services) à un autre. La portabilité implique que les personnes concernées puissent obtenir leurs données dans un format lisible par machine (voir l'art. 20(1) du RGPD) et, si cela est possible, de les faire transmettre directement d'un responsable du traitement à un autre (voir art. 20, paragraphe 2, du RGPD).

1.6.2 Articles et considérants connexes

Alors que l'art. 5(1)(f) du RGPD indique de manière abstraite que des "mesures techniques ou organisationnelles appropriées" doivent être utilisées pour mettre en œuvre les objectifs de protection de la sécurité mentionnés ci-dessus, l'**art. 32 du RGPD fournit plus de détails.**

L'article 32, paragraphe 1, dispose que, lorsqu'ils décident des mesures appropriées, les responsables du traitement tiennent compte de "l'**état de l'art** et des **coûts de mise en œuvre**", ainsi que de "la nature, la portée, le **contexte** et les finalités **du traitement**". En particulier, le contexte du traitement est pertinent ici, car on peut faire valoir que le **paysage** actuel **des menaces** en est un aspect. Comme prévu, le responsable du traitement doit également prendre en compte "**les risques pour les** droits et libertés des **personnes physiques**".

[112] L'art. 32(2) du RGPD utilise l'expression "transmis, stocké ou traité d'une autre manière".

Le niveau de protection requis dépend donc clairement de la gravité des conséquences indésirables auxquelles les personnes concernées sont exposées et d'un modèle de menace qui estime la probabilité d'événements indésirables. La sécurité n'est donc qu'un moyen, et non un objectif en soi. Le niveau de sécurité est suffisant lorsque les risques pour les personnes concernées sont ramenés à un niveau acceptable. Le choix des mesures dépend à la fois de ce que le marché a à offrir et du rapport coût-efficacité de ces mesures.

L'art. 32(1)(d) du RGPD énonce le concept bien accepté selon lequel **la sécurité est un processus**, et non une finalité réalisée une fois. En particulier, le RGPD exige "un processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement".

L'art. 32(2) du RGPD fournit des **détails supplémentaires** marginaux **sur ce qu'impliquent les objectifs de protection**, en énumérant " la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée ou l'accès aux données à caractère personnel transmises, stockées ou traitées d'une autre manière ".

L'article 32, paragraphe 3, du RGPD suggère que "[l]e respect d'un **code de conduite approuvé** ou d'un **mécanisme de certification approuvé** peut être utilisé comme un élément permettant de **démontrer le respect**" du principe d'*intégrité et de confidentialité*.

L'art. 32(4) du RGPD précise qu'un élément important de la sécurité consiste à **s'assurer que les employés n'agissent que sur instruction et selon les instructions du responsable du traitement**. Cela est nécessaire pour établir une responsabilité et une reddition de comptes claires. Il est également nécessaire de garantir l'exigence de l'art. 5(1)(f) de "protection contre le traitement non autorisé ou illicite".

De l'**Art. 25** du RGPD, il s'ensuit que toutes les exigences posées par le RGPD, y compris la sécurité, doivent être prises en compte **tout au long du cycle de vie** de l'activité de traitement. Le RGPD exige donc également la **sécurité par conception et par défaut**. La sécurité doit donc être prise en compte au début du cycle de vie, par exemple en fonction des exigences utilisées pour un appel d'offres, et à la fin du cycle de vie, par exemple lors de la migration des opérations vers un nouveau système de traitement et du démantèlement de l'ancien.

L'art. 30(1)(g) du RGPD exige d'énumérer spécifiquement les **mesures de *sécurité*** techniques et organisationnelles dans les ***registres de traitement*** qui sont destinés aux autorités de contrôle.

1.6.3 Mesures techniques et organisationnelles connexes

Les exemples suivants de mesures techniques et organisationnelles concrétisent davantage le concept de sécurité du RGPD.

1.6.3.1 Mesures en faveur de l'intégrité

- L'une des mesures techniques classiques pour soutenir l'intégrité est le **traitement transactionnel**. Il est surtout connu des systèmes de gestion de bases de données, mais il est également possible dans d'autres contextes[113] . Les transactions sont importantes lorsqu'une opération qui fait passer le système d'un état cohérent à un autre est composée de plusieurs étapes de traitement (c'est-à-dire qu'elle n'est pas "atomique"). Une transaction permet alors de s'assurer que toutes ces étapes ou

[113] Pour des exemples de traitement transactionnel en dehors des SGBD, voir par exemple https://en.wikipedia.org/wiki/Tuxedo_(software)ethttps://docs.oracle.com/cd/E13222_01/wls/docs81/jta/trxejb.html (dernière visite le 20/05/2020).

aucune ne sont appliquées, même si le système se plante en plein milieu. Elle garantit ainsi que le système reste toujours dans un état cohérent.

- Des incohérences peuvent survenir en raison d'erreurs de transmission dans des lignes de communication bruyantes. La mesure technique de **correction d'erreur avant**[114] intégrée aux protocoles de communication modernes permet de garantir l'intégrité des données pendant le transfert.
- Une mesure technique courante pour détecter les changements indésirables dans les ensembles de données utilise les **sommes de contrôle (**alias hachage ou condensé). En particulier, la somme de contrôle d'un ensemble de données est calculée lorsque l'on sait qu'il est dans un état cohérent. À un moment ultérieur, la somme de contrôle de l'ensemble de données peut être recalculée et comparée à la somme initiale afin de détecter les modifications et les altérations.
- L'intégrité est une question importante dans la distribution de logiciels, en particulier si le logiciel est téléchargé automatiquement sur un réseau. Les mises à jour automatiques des systèmes d'exploitation en sont un excellent exemple. Pour garantir l'intégrité du logiciel, des mesures techniques telles que l'**authentification des sources** sur le réseau et la **signature numérique du logiciel** sont souvent utilisées. La signature numérique est souvent utilisée aussi pour les fichiers de données.

1.6.3.2 Mesures en faveur de la confidentialité

- Une mesure organisationnelle de conception à l'appui de la confidentialité consiste à **analyser** les **conséquences** que des divulgations non souhaitées à diverses parties peuvent avoir **pour les personnes concernées**. Cette mesure est comparable à la sécurité informatique, qui consiste à identifier le patrimoine critique de l'organisation qui nécessite une protection particulière.
- La confidentialité exige que le responsable du traitement mette en œuvre des mesures de protection contre le traitement non autorisé (voir l'art. 5(1)(f) du RGPD). Comme le soulignent les art. 29 et 32(4) du RGPD, cela implique que les employés ne traitent les données à caractère personnel que sur instruction et selon les instructions du responsable du traitement. Il existe une multitude de mesures organisationnelles qui soutiennent cette exigence, notamment les suivantes :
    - **Vérification** des nouveaux employés pour s'assurer qu'ils ont les compétences nécessaires pour exécuter les instructions des responsables des données ;
    - Un moyen légal qui "garantit que les **personnes autorisées** àtraiter les données à caractère personnel se sont **engagées à respecter la confidentialité** ou sont soumises à une obligation légale de confidentialité appropriée". (Le libellé est tiré de l'art. 28, paragraphe 3, point b) qui fait référence aux personnes travaillant pour des sous-traitants, mais qui est également applicable aux personnes travaillant pour le responsable du traitement).
    - En ce sens, les **contrats avec les éventuels sous-traitants** (voir art. 28(3) du RGPD) qui transmettent des exigences de confidentialité doivent être considérés comme des mesures.
    - **Formation** des employés sur la façon d'exécuter les instructions ;

[114]Voir par exemple, https://en.wikipedia.org/wiki/Forward_error_correction (dernière visite le 20/05/2020).

- **Des points de contact internes** pour les employés qui veulent clarifier la façon d'exécuter les instructions ;
- Les manuels qui décrivent les instructions (**manuels de processus**) ;
- **Supervision** et **contrôle de la qualité**.

- Ce qui vaut pour les instructions aux ressources humaines vaut également pour les **instructions aux ressources techniques**, c'est-à-dire les logiciels. La mise en œuvre de mesures de protection contre le traitement non autorisé implique que les responsables du traitement doivent s'assurer que le logiciel correspond effectivement à leurs instructions. Il existe plusieurs mesures à cet effet, dont les suivantes :
  - **Spécification d'exigences précises** en tant que données d'entrée pour les appels d'offres ou pour le développement personnalisé de logiciels ;
  - **Test d'acceptation** formel par le responsable du traitement ;
  - **Analyse des nouvelles versions** de logiciels pour vérifier que les fonctionnalités modifiées correspondent toujours aux instructions du responsable du traitement et qu'aucune dérive fonctionnelle supplémentaire ne se produise (**dérive fonctionnelle**) correspondant à un traitement qui n'a pas été autorisé par le responsable du traitement.
- Une mesure technique importante est le **contrôle d'accès** qui permet de s'assurer que seul le personnel autorisé peut accéder aux systèmes et aux données à des fins autorisées. Le contrôle d'accès peut impliquer une multitude de mesures, dont les suivantes :
  - Délivrance d'**identifiants d'authentification**.
  - Configuration des **droits** et des conditions d'**accès**.
  - Gestion du **cycle de vie des identifiants** et des **droits d'accès**, y compris l'expiration et le renouvellement, la révocation (par exemple, lors du départ des employés), l'octroi et la révocation des droits d'accès temporaires (par exemple, lorsque les employés sont malades).
  - **Audits** réguliers de l'efficacité globale du système de contrôle d'accès.
- Il existe une multitude de mesures techniques visant à empêcher les personnes non autorisées (internes ou externes) d'accéder aux données. On parle généralement de **protection des données au repos, en transit et en cours d'utilisation.** Les deux premiers aspects nécessitent généralement un **cryptage**.
- Les mesures existantes pour empêcher les personnes non autorisées d'accéder aux systèmes et aux réseaux sont nombreuses. En voici quelques exemples :
  - **Durcissement** des systèmes d'exploitation ;
  - Application en temps utile des **correctifs et des mises à jour critiques pour la sécurité ;**
  - **Pare-feu** ;
  - Installation d'un logiciel **anti-malware** ;
  - Fonctionnement des **systèmes de détection d'intrusion** ;
- Lors du **développement de logiciels**, de nombreuses mesures sont disponibles pour empêcher l'accès non autorisé aux logiciels et aux systèmes, notamment l'assainissement des entrées, les mesures de prévention des types d'attaques connus

tels que le cross site scripting, les méthodes qui empêchent les débordements de mémoire tampon, la randomisation de la mémoire, etc.

- Certaines mesures ne permettent pas d'empêcher directement le traitement non autorisé, mais elles ont un effet **dissuasif** en aidant à **détecter** unetelle action, à **déterminer** clairement **la responsabilité** et à permettre de demander **des comptes aux personnes** qui ont agi sans autorisation. Ces mesures impliquent généralement la **journalisation** ou la création de **pistes d'audit**.
- Une mesure importante associée à la **fin de vie** des composants de stockage comprend la **destruction** complète et **sécurisée** de toutes les données avant **leur élimination**.

1.6.3.3 Mesures en faveur de la disponibilité et de la résilience

- L'analyse de l'impact d'une perte accidentelle sur les personnes concernées constitue une mesure organisationnelle de conception. Elle vise à identifier le patrimoine qui doit être protégé par des mesures de disponibilité.
- Une autre mesure du temps de conception concerne la portabilité des données et examine la disponibilité de formats normalisés appropriés lisibles par machine et les possibilités de transférer automatiquement les données à un autre responsable du traitement (voir l'art. 20(2) du RGPD).
- **La redondance du stockage** est un type de mesure très courant en faveur de la disponibilité. Voici quelques exemples bien connus :
  - Stockage RAID ;
  - Sauvegardes ;
  - Stockage à distance à l'appui de la reprise après sinistre.
- Au-delà du stockage des données, la **redondance** peut également être importante **dans les systèmes de traitement**. Les mesures correspondantes sont les suivantes :
  - Configurations maître/esclave avec basculement ;
  - Fermes de serveurs et configurations en nuage ;
  - Stratégies de migration de processus basées sur la virtualisation.

1.7 Responsabilité

Bud P. Bruegger (ULD)

Remerciements : L'auteur remercie Johann Čas et Walter Peissl (tous deux de l'OEAW) pour leur contribution à l'analyse de ce principe, qui a servi de base à la description présentée ici.

Les paragraphes suivants traitent du principe de *responsabilité* défini à l'art. 5(2) du RGPD.

***La responsabilité* en quelques mots :**

La responsabilité consiste en deux exigences pour les responsables du traitement :

- **Respect** des principes du RGPD ;
- **Démonstration de la conformité.**

La **conformité** est obtenue en mettant en œuvre des ***mesures techniques et organisationnelles*** qui sont adéquates par rapport aux risques pour les droits et libertés des personnes concernées, qui correspondent à l'état de l'art de la technologie et qui sont rentables. Chaque description des principes a fourni des exemples de telles mesures techniques et organisationnelles. Pour une application systématique de ces mesures, les responsables du traitement peuvent créer des ***politiques de protection des données***. Les ***codes de conduite approuvés***, lorsqu'ils existent, sont similaires mais sont pré-approuvés et s'adressent généralement à un secteur entier. La conformité n'est pas un état que l'on atteint une fois, mais **un processus continu** qui s'étend sur tout le cycle de vie d'une activité de traitement.

La **démonstration de la conformité** sefait principalement par la **documentation** (voir la section "Documentation du traitement" dans "Principaux outils et actions"). La documentation doit être continue comme le processus de conformité. Chaque mesure mise en œuvre, y compris les considérations et les décisions relatives à la protection des données, doit être documentée. Le RGPD exige deux documents formels pour démontrer la conformité aux *autorités de contrôle* : le ***registre des traitements*** (voir "Documentation du traitement" pour plus de détails) et, lorsque les risques sont susceptibles d'être élevés, une ***analyse d'impact sur la protection des données*** (voir la section du même nom dans "Principaux outils et actions" dans la partie II pour plus de détails). La *certification* peut aider à démontrer la conformité.

1.7.1 Description

Dans la section "Comprendre la protection des données : le règlement européen en quelques mots" ci-dessus, la *responsabilité* totale des responsables du traitement a été présentée comme la première de plusieurs mesures prises par le RGPD pour limiter le pouvoir acquis par le responsable du traitement par le biais du traitement et l'équilibrer avec le pouvoir des personnes concernées. Voir la section 1.6.1 "Les responsables du traitement sont pleinement responsables" pour plus de détails.

Le RGPD définit ce principe comme suit :

Définition de l'art. 5(2) du RGPD :

Le **responsable du traitement** doit être **responsable du respect** du paragraphe 1 ("*responsabilité")* et être en mesure d'en **apporter la preuve**.

Le paragraphe 1 fait ici référence aux principes qui ont été discutés dans les six sections précédentes, à savoir

- Licéité, loyauté et transparence ;
- Limitation de l'objectif ;
- Minimisation des données ;
- Précision ;
- Limitation du stockage ; et
- Intégrité et confidentialité.

Pour reformuler l'art. 5(2), le **responsable du traitement** est pleinement **responsable de** deux choses :

- **Le respect** de ces six principes,
- **Démontrer la conformité**.

La responsabilité n'est donc pas un nouveau principe auquel les responsables du traitement doivent se conformer, mais elle indique aux responsables du traitement **comment appliquer les six principes**.

Notez que le fait de devoir démontrer la conformité est un grand pas au-delà de la simple obligation de se conformer. En particulier, il fait peser la "charge de la preuve" sur le responsable du traitement ; un responsable du traitement qui ne peut ou ne veut pas démontrer sa conformité est en violation du RGPD.

1.7.1.1 Qu'est-ce que cela signifie de se conformer ?

Alors que l'art. 5(2) ne parle que du respect des six principes, il doit en fait être étendu à l'**ensemble du RGPD**. Ceci est motivé par le fait que tous les autres articles ont pour but de détailler les principes ou de décrire plus en détail la manière dont ils doivent être mis en œuvre.

Dans tout le RGPD, il n'y a qu'une seule façon de se mettre en conformité, à savoir par la mise en œuvre de **mesures techniques ou organisationnelles**. Dans l'Art. 24, qui décrit les obligations d'un responsable du traitement, le premier paragraphe indique explicitement que c'est ainsi que les responsables du traitement se conforment (et démontrent leur conformité) au RGPD ; l'art. 25(1) stipule que la protection des données dès la conception se résume à la mise en œuvre de telles mesures tout au long du cycle de vie de l'activité de traitement ; l'art. 25(2) met également l'accent sur l'utilisation de telles mesures pour la protection des données par défaut ; l'art. 28(1) stipule que les sous-traitants doivent également mettre en œuvre de telles mesures ; l'art. 32 stipule que le respect des exigences en matière de sécurité est également assuré par la mise en œuvre de telles mesures ; et l'art. 89(1) stipule que les garanties nécessaires pour le "traitement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques" garantissent que de telles mesures sont en place.

Étant donné que les mesures techniques et organisationnelles sont si essentielles pour assurer la conformité, la discussion de chacun des six principes ci-dessus s'est terminée par des exemples de telles mesures.

Le respect des exigences en matière de protection des données peut être considéré comme un processus. Conformément au concept de *protection des données dès la conception* (voir l'art. 25(1) du RGPD), dans chaque phase du cycle de vie de l'activité de traitement, les risques pour les droits et libertés des personnes physiques sont évalués et des mesures d'atténuation appropriées sont mises en œuvre. Le RGPD utilise une définition très large du terme "*mesures techniques et organisationnelles"*. Elle comprend essentiellement tout ce qu'un responsable du traitement fait pour se conformer au RGPD. Par conséquent, même l'étape d'évaluation mentionnée ci-dessus peut être considérée comme une mesure en soi.

1.7.1.2 Qu'est-ce que cela signifie de démontrer la conformité ?

Étant donné que la conformité est obtenue par la mise en œuvre de mesures appropriées, il n'est pas surprenant que la **démonstration de la conformité documente ces mesures**.

Cela ressort par exemple de l'art. 30(1)(g) qui impose d'énumérer les mesures pertinentes pour la sécurité dans les ***registres de traitement***. Il est également central dans l'art. 35 sur l'**analyse d'impact sur la protection des données**, qui est sans doute le principal outil prévu par le RGPD pour démontrer la conformité. En particulier, l'art. 35(7)(d) demande aux responsables du traitement de déclarer les mesures qu'ils ont mises en œuvre pour assurer la protection des données à caractère personnel et démontrer leur conformité au RGPD.

Une **discussion plus détaillée** de la **documentation du traitement** en général, et des analyses d'impact sur la protection des données en particulier, se trouve dans la section "Principaux outils et actions" ci-dessous. Ces deux sections soulignent l'importance des mesures techniques et organisationnelles.

1.7.1.3 Économie d'échelle pour la conformité et sa démonstration

Comme indiqué ci-dessus, la conformité est obtenue par la mise en œuvre de mesures techniques et organisationnelles. Il ressort clairement de la discussion ci-dessus que la conformité peut nécessiter un nombre important de ces mesures. Cela peut rendre plus difficile l'évaluation de la protection réelle offerte par ces mesures et la question de savoir si cette protection est appliquée de manière uniforme et cohérente.

Pour atténuer cette difficulté, le RGPD propose certains types de "mécanismes d'abstraction" qui permettent de considérer un ensemble de mesures connexes comme une seule unité. En particulier, le RGPD prévoit deux mécanismes de ce type dans son art. 24 qui décrit la "responsabilité du responsable du traitement" :

- ***Les politiques de protection des données*** (voir art. 24(2) du RGPD), et
- ***codes de conduite approuvés*** (voir art. 24(3) et 40).

Une ***politique de protection des données*** est un mécanisme qui rend l'application des mesures systématique. Cela garantit un ensemble uniforme et cohérent de mesures dans des situations similaires. Par exemple, au lieu de devoir évaluer quelles mesures de sécurité sont appropriées pour chacun des nombreux serveurs très similaires, une politique unique peut être rédigée une fois et appliquée à tous les serveurs. De toute évidence, en particulier dans les opérations de traitement complexes et étendues, cela permet de réaliser des économies d'échelle potentiellement très importantes, qui peuvent même couvrir plusieurs activités de traitement indépendantes du même responsable du traitement.

Le mécanisme des ***codes de conduite approuvés*** étend cette économie d'échelle, au-delà d'un seul responsable de traitement, à tout un secteur de transformation. Ces codes de conduite sont élaborés par des **associations** et autres organismes **représentant des catégories de responsables de traitement ou de sous-traitants** (voir art. 40(2) du RGPD). Lorsqu'un code de conduite ne concerne pas des activités de traitement dans plusieurs États membres, l'*autorité de contrôle* compétente peut l'**approuver** (voir l'art. 40(5) du RGPD), puis l'enregistrer et le publier (voir l'art. 40(6) du RGPD). Lorsqu'un projet de code de conduite concerne des activités de traitement dans plusieurs États membres, un processus similaire est utilisé, qui implique le Conseil européen de la protection des données (voir l'art. 40(7) du RGPD). Il est évident que les codes de conduite permettent également une économie d'échelle aux autorités de contrôle qui doivent surveiller le respect du RGPD.

Tant les *codes de conduite approuvés* que la *certification* (conformément à l'article 42 du RGPD) peuvent aider les responsables du traitement à démontrer leur conformité (voir l'article 24, paragraphe 3, du RGPD).

1.7.2 Articles et considérants connexes

La responsabilité concerne la conformité et la démonstration de la conformité. Elle fait directement référence aux six principes de la protection des données définis à l'art. 5(1) mais s'étend indirectement à l'ensemble du RGPD.

L'art. 24 du RGPD fournit des détails sur la manière dont un responsable du traitement doit atteindre la conformité et la démontrer. L'art. 25(1) sur la protection des données dès la conception illustre comment la conformité (et par conséquent sa démonstration) doit être considérée comme un processus continu qui couvre tous les cycles de vie d'une activité de traitement. Les *codes de conduite* et la *certification* qui peuvent contribuer à la conformité et à sa certification sont décrits aux art. 40 et 42 du RGPD, respectivement.

Les articles particulièrement pertinents pour la démonstration de la conformité sont les articles 30 *"Registres de traitement"* et 35 "*Analyse d'impact sur la protection des données"*.

1.7.3 Mesures techniques et organisationnelles connexes

Les mesures pertinentes pour la *responsabilisation* portent sur la manière d'assurer la conformité et sa démonstration, plutôt que sur ce qui doit être fait pour se conformer.

Les méta-mesures suivantes traitent des moyens d'**assurer la conformité** :

- ***La protection des données dès la conception et par défaut*** (voir article 25 du RGPD),
- ***L'analyse d'impact sur la protection des données*** (voir l'article 35 du RGPD) dans sa fonction de processus continu qui guide le responsable du traitement dans l'évaluation des risques et l'identification des mesures techniques et organisationnelles appropriées pour les atténuer.
- La création et l'application de ***politiques de protection des données*** (voir art. 24(2) du RGPD).
- L'adhésion à des ***codes de conduite approuvés*** (voir art. 24(3) du RGPD).
- L'adhésion à des ***mécanismes de certification approuvés*** (voir art. 24(3) du RGPD).

Les mesures "méta" suivantes portent sur les moyens de **documenter la conformité** :

- L'***analyse d'impact sur la protection des données*** (voir article 35 du RGPD) dans sa fonction de rapport. Lorsque le risque n'est pas susceptible d'être élevé et qu'une telle analyse d'impact n'est donc pas nécessaire, il convient de documenter la manière dont cette estimation du risque a été établie (voir la section "Analyse d'impact sur la protection des données″ dans "Principaux outils et actions" de la partie II des présentes lignes directrices pour plus de détails).
- Les ***registres de traitement*** (voir article 30 du RGPD).